QATAR UNIVERSITY

COLLEGE OF ENGINEERING

CYBERSECURITY ENABLED PROTECTION AND OPTIMIZATION OF ACTIVE DISTRIBUTION NETWORKS IN SMART GRIDS

BY

SHAHBAZ HUSSAIN

A Dissertation Submitted to

the College of Engineering

in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy in Electrical Engineering

January 2023

© 2023 Shahbaz Hussain. All Rights Reserved.

COMMITTEE PAGE

The members of the Committee approve the Dissertation of

Shahbaz Hussain defended on 17/11/2022.

_____

Prof. Atif Iqbal

Thesis/Dissertation Supervisor

_____

Prof. Stefano Zanero

Thesis/Dissertation Supervisor

_____

Prof. Rashid Alammari

Thesis/Dissertation Co-Supervisor

_____

Prof. Abdullatif Shikfa

Thesis/Dissertation Co-Supervisor

_____

Prof. Enrico Ragini

Thesis/Dissertation Co-Supervisor

_____

Dr. Hasan Mehrjerdi

Committee Member

Approved:

_____

Khalid Kamal Naji, Dean, College of Engineering

ABSTRACT

Shahbaz Hussain, Doctorate: January: 2023,

Doctorate of Philosophy in Electrical Engineering

Title: Cybersecurity enabled protection and optimization of active distribution networks in smart grids

Supervisor of Dissertation: Atif Iqbal, Stefano Zanero.

Co-Supervisor of Dissertation: Rashid Alammari, Abdullatif Shikfa, Enrico Ragaini.

The electrical grid is evolving into smart grid with the integration of renewables and the evolution of advanced information and communication technology (ICT). This enables remote monitoring and control for operators in power system on the one hand, but on the other hand it has opened doors for attackers to intrude from cyberspace. Hence, there is a requirement of protection, optimization and cybersecurity of both conventional and smart grids. This work deals with the classical problem of conventional grid using modern optimization techniques and develops cybersecurity solution for smart grid communication protocols in active distribution networks.

In a conventional grid, combined economic and emission dispatch is a classical problem which is tackled by particle swarm optimization and genetic algorithms and their comparison results are presented. Then the work deals with the optimal sizing of an independent renewable energy based system i.e. photovoltaic-wind turbine-battery energy storage system (PV-WT-BESS) using a novel technique called iterative filter selection approach and the results are compared with an existing technique in the literature.

In smart grids domain, the vulnerabilities and countermeasures in electrical substations are reviewed. The work is then advanced on a standard microgrid and its communication protocols i.e. Generic Object Oriented Substation Events (GOOSE) and

Sampled Measure Values (SMV or simply SV) are analyzed and exploited to provide a novel cybersecurity solution. The two communication protocols are based on the IEC-61850 standard and are used to control breakers through protection and control IEDs and collect sampled values of nodal currents and voltages through merging units respectively.

Both GOOSE and SV are of primary importance in the IEC-61850 standard and are considered in our work both on communication and electrical levels to devise a hybrid and novel cybersecurity solution in both the information technology (IT) and operational technology (OT) domain. The standard case considered in our work is a Banshee microgrid and its simulation, false data injection (FDI) attacks in the form of replay and masquerade attacks and then the novel cybersecurity methodology to counter such attacks are done in real time digital simulator (RTDS) in conjunction with a couple of open source tools.

DEDICATION

To my family, who supported me throughout the duration of my studies.

ACKNOWLEDGMENTS

First and foremost, I would like to thank my supervisors, Prof. Atif Iqbal and Prof. Stefano Zanero to provide helpful guidance and feedback throughout my doctoral studies. I would like to thank Prof. Rashid Alammari, Prof. Abdullatif Shikfa and Prof. Enrico Ragaini, my co-supervisors, for their valuable guidance and countless support. Prof. Atif is always available for discussion, which helps me to achieve my research objectives.

I also thank Dr. S. M. Suhail Hussain for his positive feedbacks and input to the research work, Mr. M. Waqas for his motivation to complete the thesis report way before the deadline and Dr. Shoaib Mallick for sharing the thesis template and three of them in developing a friendly and dynamic atmosphere.

A special thanks to a loving parent, my mother Mrs. Hanifan Bibi and my siblings (Mr. Ishtiaq Hussain, Mr. Sheraz Hussain and Mrs. Sadia Hussain) and my late wife Mrs. Maria Fazal for their love, encouragement, countless and unconditional support throughout my studies. They help me and supported me every time. My close cousins Mr. Abrar Hussain and Mr. Zia-ul-Islam have been the source of wise advices whenever I require on life and studies throughout my career. Last but not the least, the role of my deceased father Mr. Nazar Hussain is pivotal as he always encouraged me in his life to go for higher studies and pursue higher goals even before my admission into MS and PhD programs.

TABLE OF CONTENT

DEDICATION v

ACKNOWLEDGMENTS vi

LIST OF TABLES xi

LIST OF FIGURES xiii

CHAPTER 1: INTRODUCTION 1

1.1. Combined Economic and Emission Dispatch (CEED) of an independent power plant: 1

1.2. Optimal sizing of photovoltaic-wind turbine-battery energy storage system (PV-WT-BESS): 2

1.3. IEC-61850 universal automation standard and communication protocols: 2

1.4. RTDS, FDI attacks and open source tools: 2

1.5. Information technology (IT) and operational technology (OT) based cybersecurity: 3

1.6. Motivation and Background: 4

1.7. Research Problem: 4

1.8. Research Objectives: 4

1.9. Main Contribution: 5

1.10. Thesis organization: 5

CHAPTER 2: LITERATURE REVIEW 7

2.1. Combined Economic Emission Dispatch 7

2.2. Optimal sizing of standalone renewable energy based (PV-WT-BESS)

system: 12

2.3. Vulnerabilities and Countermeasures in Electrical Substations: 13

2.3.1. Background 17

2.3.2. Evolution of electrical substations 23

2.3.3. Cyber security concerns in the energy sector 32

2.3.4. Cyberattacks on electrical substations 43

2.3.5. Countermeasures development for electrical substations 58

2.3.6. Cybersecurity solution for electrical substations 69

2.3.7. Summary 73

CHAPTER 3: IMPLEMENTATION AND COMPARISON OF PARTICLE SWARM OPTIMIZATION AND GENETIC ALGORITHM TECHNIQUES IN COMBINED ECONOMIC EMISSION DISPATCH OF AN INDEPENDENT POWER PLANT 75

3.1. Introduction: 75

3.2. Problem Formulation: 75

3.3. Implementation of PSO to CEED: 78

3.4. Implementation of GA to CEED: 81

3.5. Simulation Results: 85

3.5.1. IEEE 30 Bus System: 86

3.5.2. Pakistani IPP: 88

3.6. Results Discussion: 91

3.7. Summary: 93

CHAPTER 4: OPTIMIZATION OF HYBRID RENEWABLE ENERGY SYSTEM USING ITERATIVE FILTER SELECTION APPROACH 94

4.1. Introduction: 94

4.2. Hybrid renewable system configuration: 94

4.3. Problem formulation: 97

4.3.1. Total cost: 97

4.3.2. Reliability and Dump load sizing: 98

4.4. Iterative filter selection approach: 99

4.5. Results and Discussion: 102

4.6. Summary: 107

CHAPTER 5: A NOVEL HYBRID METHODOLOGY TO SECURE GOOSE MESSAGES AGAINST CYBERATTACKS IN SMART GRIDS 108

5.1. Introduction: 108

5.2. IEC 61850 Protocols and Control Authority: 112

5.3. Methodology to Validate Cyberattacks: 115

5.3.1. Testbed for implementation and modification of IEC 61850 communication 115

5.3.2. Simulation and modification of GOOSE packets 117

5.3.3. Impact of FDI attacks on Simple and Complex Electrical Systems 120

5.4. Implementation of Hybrid Solution: 125

5.4.1. Sequence or Communication Module (COMM): 129

5.4.2. Content or Electrical Module (ELEC): 129

5.5. Summary: 132

CHAPTER 6: AMELIORATION OF CYBERATTACKS ON SAMPLED VALUES IN AUTOMATED POWER SYSTEMS USING A NOVEL SEQUENCE CONTENT RESOLVER 133

6.1. Introduction: 133

6.2. Cyberattacks on the SV Protocol and Impact on Electrical Network: 139

6.3. Proposed Mitigation Strategy: 142

6.4. Simulation Results and Discussion: 144

6.4.1. Cyberattack on SV Packets 145

6.4.2. Evaluation of Impact on Electrical Side 149

6.4.3. Implementation of Proposed Solution 152

6.4.4. Performance Evaluation 157

6.5. Summary: 159

CHAPTER 7: Conclusion and Future work: 161

References: 165

LIST OF TABLES

Table 2-1. Best optimization methods employed in different systems with regard to cost, emission, and time 11

Table 2-2. Contents of IEC 61850 standard [47] 29

Table 2-3. IEC-61850 communication delay requirements [106] 47

Table 2-4. Taxonomy of cyberattacks for electrical substations. 56

Table 2-5. Characteristics of custom made countermeasures in reported literature 66

Table 2-6. Countermeasures with attack type in electrical substations corresponding to taxonomy of attacks with AVD model. 67

Table 3-1. The types of crossover. 83

Table 3-2. The real-time simulation results of PSO and GA for IEEE 30 bus system with P_D = 1500 MW and P_D = 2000 MW. 87

Table 3-3. The real-time simulation results of PSO and GA for Pakistani independent power plant (IPP) with P_D = 500 MW and P_D = 700 MW. 90

Table 4-1. The best compromised hybrid system by iterative filter selection approach and comparison with iterative-pareto-fuzzy and particle swarm optimization techniques 104

Table 4-2. The process of determining the best possible combination for PV-WT-battery system using iterative filter selection approach 105

Table 5-1. Cybersecurity solutions for securing GOOSE message 111

Table 5-2. Logical node classes and control parameters as per IEC-61850 113

Table 5-3. Switchgear control based on control authority 114

Table 5-4. Voltage before and after tripping on source and load buses 121

Table 6-1. Comparison of main feeder breaker tripping, before and after, in the three areas of microgrid 152

Table 6-2. Cybersecurity solutions provided in literature on SV packets 157

Table 6-3. Computational delays of cybersecurity mechanism for SV packets 159

LIST OF FIGURES

Figure 2-1. Optimization methods. 8

Figure 2-2. Evolution of power grids [46] 16

Figure 2-3. Substation automation model [47] 19

Figure 2-4. Intruder attack [79]. 21

Figure 2-5. Schematic of traditional substation [83] 25

Figure 2-6. Substation automation model [57] 26

Figure 2-7. Schematic of digital substation [84] 27

Figure 2-8. Model showing IEC 61850 communication layers [47] 31

Figure 2-9. Architecture of IEC TC57 communication standards [93] 32

Figure 2-10. Comprehensive Attack-Vulnerability-Damage (AVD) model 35

Figure 2-11. Schematic showing different potential attacks on a power grid [102] 37

Figure 2-12. Attack scenarios [67]. 41

Figure 2-13. SCADA infrastructure [104]. 42

Figure 2-14. Transformer 1 overloading [104]. 42

Figure 2-15. Substation outage [104]. 43

Figure 2-16. Communication network of a power system [49] 45

Figure 2-17. Data model in IEC 61850 [91] 51

Figure 2-18. Ethernet data frame [53] 53

Figure 2-19. Changing status of IED in LN hierarchy [114] 54

Figure 2-20. Countermeasures to substation's network attacks 60

Figure 2-21. Countermeasures to substation's data attacks 62

Figure 2-22. IED protection with embedded IDS [54]. 63

Figure 2-23. Countermeasures to substation's devices attacks 64

Figure 2-24. Physical and cyber layers in a substation [97]. 70

Figure 2-25. Cybersecurity protection system [130]. 73

Figure 3-1. Implementation of combined economic emission dispatch (CEED) using particle swarm optimization (PSO) algorithm. 81

Figure 3-2. Implementation of CEED using genetic algorithm (GA) algorithm. 85

Figure 3-3. The convergence characteristics of PSO and GA with regard to fuel cost and emission for IEEE 30 bus system with P_D = 1500 MW. 88

Figure 3-4. The convergence characteristics of PSO and GA with regard to fuel cost and emission for IEEE 30 bus system with P_D = 2000 MW. 88

Figure 3-5. The convergence characteristics of PSO and GA with regard to fuel cost and emission for Pakistani IPP with P_D = 500 MW. 91

Figure 3-6. The convergence characteristics of PSO and GA with regard to fuel cost and emission for Pakistani IPP with P_D = 700 MW. 91

Figure 4-1. Stand-alone hybrid PV-WT-battery configuration.....95

Figure 4-2. Flowchart for iterative filter selection approach applied for optimal design of hybrid renewable energy system 101

Figure 4-3. The initial iterative points using filter selection approach without the application of filters 102

Figure 4-4. The pareto points for 90% reliability using iterative-pareto-fuzzy technique 103

Figure 5-1. Circuit breaker control based on switch object 113

Figure 5-2. Testbed with RTDS, Snort, and Wireshark.....117

Figure 5-3. RTDS runtime for GOOSE communication between IED 1 and IED 2 before the manipulation of packets by the attacker 118

Figure 5-4. RTDS runtime for GOOSE communication between IED 1 and IED 2 after the manipulation of packets by the attacker.....119

Figure 5-5. Original and counterfeit GOOSE packets for IED 1 on LAN port 120
Figure 5-6. 3-phase doubly fed system in RSCAD Draft with 3 buses, circuit breaker, isolators and load 121
Figure 5-7. Runtime single line diagram of Banshee microgrid.....122
Figure 5-8. Islanding Area 1 or Area 3 vs. Area 2.....124
Figure 5-9. Block diagram of Sequence Content Resolver (hybrid solution).....126
Figure 5-10. Attack tree showing the paths for potential cyberattacks [150]. 127
Figure 5-11. Functional diagram of novel sequence content resolver for GOOSE communication packets.....130
Figure 5-12. Original GOOSE packets for IED 1 on LAN port with sequence content resolver.....132
Figure 6-1. FDI attack on P&C IED (direct route via GOOSE) and on MU IED (indirect route via SV). 135
Figure 6-2. Structure of SV packet. 141
Figure 6-3. SV packet frame in Wireshark 141
Figure 6-4. Devices at station, bay and process levels in a substation. 142
Figure 6-5. Block diagram of Sequence Content Resolver.....144
Figure 6-6. Testbed with RTDS, Wireshark and Snort.....145
Figure 6-7. Swapping of packets in Wireshark (a) packet with smpCnt = 214 should appear after the (b). (c) Dropping of packets in Wirashark (packets after smpCnt = 222 are dropped). 146
Figure 6-8. 3-phase current waveform at input of publisher (top) and received by subscriber (bottom) after attack. 147
Figure 6-9. 3-phase voltage waveform at input of publisher (top) and received by subscriber (bottom) after attack. 148

Figure 6-10. FDI attack (replay and masquearde) on data items of SV packets; left is the original packet while right is the packet after attack where all values are modified. 149
Figure 6-11. Runtime single line diagram of Banshee microgrid in RTDS. 151
Figure 6-12. Functional diagram of Sequence Content Resolver 154
Figure 6-13. 3-phase current waveform at input of publisher (top) and received sampled waveform by subscriber (bottom) after mitigating the attack. 155
Figure 6-14. 3-phase voltage waveform at input of publisher (top) and received sampled waveform by subscriber (bottom) after mitigating the attack. 156
Figure 6-15. Normal SV packets in Wireshark after mitigating the attack. 156
Figure 6-16. SV message exchange between a publisher and a subscriber. 158

CHAPTER 1: INTRODUCTION

The conventional grid has classical problem such as economic load dispatch where artificial intelligence models such as particle swarm optimization and genetic algorithm can be introduced. In renewable energy based microgrid also, advanced intelligent techniques to resolve the optimal sizing of the system can be applied. Moving towards the smart grids, there is an automation IEC-61850 standard whose communication protocols can be studied upon a standard Banshee microgrid connected to main grid having both conventional and renewable generation. The microgrid can be simulated in a real time digital simulator (RTDS) and the communication protocols can be exploited by false data injection (FDI) attacks with open source tools to devise novel cybersecurity methodologies. In the IEC-61850 standard, GOOSE and SV are the time stringent protocols and is considered to induce FDI attacks on the protocols and later deploy cybersecurity solutions.

1.1. Combined Economic and Emission Dispatch (CEED) of an independent power plant:

In conventional grid, there are independent power producers (IPPs) which contribute their generation to the main grid. IPPs are mostly thermal based and they include numerous generators to dispatch in order to feed the desired load demand. This is called economic load dispatch and it becomes combined economic emission dispatch when both the fuel cost and emission of gases from the generators under consideration have to be optimized. For low quantity of generators, human led decision can work but for large quantity, artificial intelligence based such as particle swarm optimization and genetic algorithm can work wonders. Hence, optimization algorithms can deal with multi-objectives optimization i.e. fuel and emission of generators in a thermal power

plant.

1.2. Optimal sizing of photovoltaic-wind turbine-battery energy storage system (PV-WT-BESS):

The standalone renewable energy based system i.e. PV-WT-BESS requires optimal sizing for configuration, commissioning and installation at sites far from the main grid. This optimal sizing depends upon consideration of design objectives such as minimum cost, maximum reliability and minimum dump load. This is again a multi-objective optimization problem and can be dealt with modern algorithms based on artificial intelligence such as particle swarm optimization or fuzzy logic or some other novel technique.

1.3. IEC-61850 universal automation standard and communication protocols:

IEC-61850 is emerging as a universal automation standard for substations and beyond in power systems with the advent of information technology. This standard involves communication protocols for different functions between intelligent electronic devices (IEDs) and the famous protocols are defined below:

1) GOOSE for switching signals from IEDs to circuit breakers (CBs);
2) Sampled measured values (SMV) for measurement values from merging units (MU) to IEDs;
3) Manufacturing message specification (MMS) to exchange measurement readings and control commands between human machine interface (HMI) and IEDs; and
4) Simple network time protocols (SNTP) for time synchronization of IEDs with GPS master clock.

1.4. RTDS, FDI attacks and open source tools:

RTDS is a parallel processing hardware with RSCAD as its counterpart software brought together in 1980s for digital simulation of power systems in real time. It is manufactured by Winnipeg, Canada and they are the pioneer in real time digital simulation. The application areas of RTDS has been nowadays widely extended to:

1. Distribution
2. Smart Grid
3. Power Electronics
4. Protection

Hence to study smart grids in real time, RTDS is the perfect innovative tool with its hardware/software package. Our work is focused on the GOOSE and SV communication protocols in microgrids where messages and packets based on these protocols using RTDS are simulated. In order to simulate FDI attacks on these protocols, an open source tool by the name Snort is used and then to monitor the packets, another open source tool known as Wireshark is used.

1.5. Information technology (IT) and operational technology (OT) based cybersecurity:

In present literature [xx], researchers are more focused on IT based cybersecurity in power systems that deals only with the communication aspect of the problem. Hence, there is a requirement on more holistic solutions considering the electrical side or the OT domain of smart grid. As our focus is on GOOSE and SV protocols, so in this regards, it is required to not only check the sequence of packets and secure them but there is also a need to check the content of the messages with electrical understanding and based on this information, hybrid and holistic cybersecurity strategies are to be devised to bridge the research gap present in contemporary literature.

1.6. Motivation and Background:

As there are areas in conventional, renewable and smart grid, where modern artificial intelligence methods or holistic cybersecurity methodologies are to be deployed, hence this is the motivation and background of our research to address the research gaps, identify the classical problems in all these three areas in order to apply artificial intelligence based self-healing techniques.

1.7. Research Problem:

The research problem in our case spans over three different areas i.e. conventional, renewable and smart grid. In conventional grid, the classical combined economic emission dispatch problem is looked into with the help and comparison of two famous swarm intelligence based techniques on an independent power plant. In renewable energy based grid, the optimal sizing issue of PV-WT-BESS based configuration is delved into in order to optimize three design objectives i.e. cost, reliability and dump load by using a novel method and comparing its results with contemporary approaches. In smart grid, IEC-61850 standard based communication protocols (GOOSE and SV) in a microgrid have been worked upon using RTDS and open source tools to devise holistic cybersecurity solutions.

1.8. Research Objectives:

Starting with the conventional grid, the objective is to implement the CEED problem of an independent power plant in MATLAB using and comparing the results of particle swarm optimization and genetic algorithm. Moving towards the renewables, the objective is to optimize the cost, reliability and dump load in MATLAB by inventing a novel and better technique named as iterative-filter-selection (IFS) approach. Ending with the smart grid, the objective is to study microgrid in RTDS from GOOSE and SV

perspective, launch FDI attacks on them and deploy novel cybersecurity solutions.

1.9. Main Contribution:

This research work has the following specific contribution to the body of knowledge:

- In conventional grid, the combined economic emission dispatch of an independent power plant is implemented using two pioneer swarm intelligence techniques i.e. particle swarm optimization and genetic algorithm and together with the contribution of their implementation and comparison on the same systems, it is concluded that the former performs better to optimize the fuel cost and gases emission of generators.
- In renewables, the optimal sizing configuration problem is tackled and a novel technique is contributed which is more simple and efficient to deal with the multi-objective optimization of cost, reliability and dump load in a PV-WT-BESS configuration.
- In smart grid, the microgrid in grid connected and islanded modes is studied in RTDS to exploit GOOSE protocol in IEC-61850 standard with FDI attack and a rule based cybersecurity solution is contributed which considers the holistic perspective of IT and OT domains.
- In smart grid, the microgrid in grid connected and islanded modes is studied in RTDS to exploit SV protocol in IEC-61850 standard with FDI attack and a rule based cybersecurity solution is contributed which considers the holistic perspective of IT and OT domains.

1.10. Thesis organization:

The dissertation has been organized into the following chapters:

- Chapter 1 covers the introduction of the work under consideration. The chapter

also illustrates the research problem, outlines the research objectives, and presents the contribution of this dissertation.

- Chapter 2 covers a literature review of the problems being tackled and identifies the research gaps.
- Chapter 3 presents implementation and comparison of particle swarm optimization and genetic algorithm techniques in combined economic emission dispatch of an independent power plant.
- Chapter 4 presents optimization of hybrid renewable energy system using iterative filter selection approach.
- Chapter 5 presents a novel hybrid methodology to secure GOOSE messages against cyberattacks in smart grids.
- Chapter 6 presents amelioration of cyberattacks on sampled values in automated power systems using a novel sequence content resolver.
- Chapter 7 summarizes the research work presented in this thesis and provide the future aspect of this research work.

CHAPTER 2: LITERATURE REVIEW

In this chapter, the different methods applied in literature to solve economic emission dispatch problem will be investigated. The next section will focus on the optimal sizing issue of a standalone renewable energy based system using techniques deployed in the literature. Finally, the vulnerabilities and countermeasures in electrical substations will be discussed that are present and can be employed respectively.

2.1. Combined Economic Emission Dispatch

The primary objective of an independent electric power producer is to generate electricity at the minimum possible cost. The most expensive commodity in a thermal power plant is the fuel used for the generators to produce electricity. Hence, the focus is on minimizing the production cost; which can be achieved by dispatching the committed generators in the most economical way possible without violating the generators and system electrical constraints and ratings. Moreover, environmental regulatory authorities also impose certain limits on all gas emission sources because of the alarming situation of pollution in the past few decades of many regions around the world [1]. Therefore, a simultaneous minimization of both fuel cost and emission is the obvious way to address those challenges; hence, the idea of a combined economic emission dispatch (CEED) emerged.

Combined dispatch is an efficient and economical solution for decreasing both fuel cost and emission in a thermal power plant without the need to modify the existing system. The simulation gives flexibility to the operator to set the output of generators to achieve a fuel cost benefit for the company and emission allowed by the environmental regulatory authorities. There are many optimization techniques being employed to solve multiobjective problems like CEED. Conventional methods are

based on mathematical iterative search which are accurate but time consuming. The nonconventional methods are naturally inspired and give better, if not the best, solution in lesser time as compared to conventional methods. From these artificial-intelligence-based methods, a process of hybridization is going on to accumulate the qualities of individual methods into their hybrids counterparts. This categorization is shown in Figure 2-1 [2].

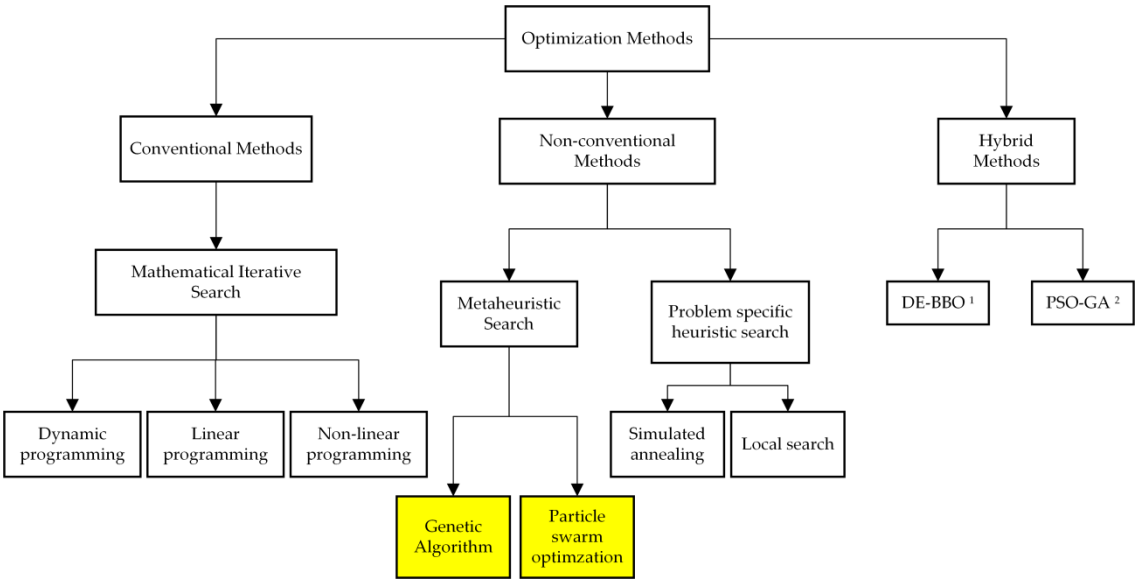


Figure 2-1**.** Optimization methods.

[1] Differential Evolution-Biogeography Based Optimization.

[2] Particle Swarm Optimization-Genetic Algorithm.

Many modern artificial intelligence (AI) techniques based on the theory of Darwinian evolution of biological organisms, e.g., genetic algorithm (GA), and social behaviors of species, e.g., particle swarm optimization (PSO), have been invented. They have been very successful concerning results and regarding dealing with the complexities occurred in formulating such problems. Particle swarm optimization and genetic algorithm are the two leading methods from AI area and are being exploited widely in every discipline including power systems [3-6]. Their hybrid versions are also

reported in the literature [7-9], where qualities of both are combined to solve a particular problem. They have also been employed individually on other problems [10, 11] where PSO was found to have better performance than that of GA.

In recently reported literature, E. Gonçalves et al. solved nonsmooth CEED using a deterministic approach with improved performance and Pareto curves [1]. They included valve point loading effect but the same approach has to be extended considering other constraints like network losses and prohibited operating zones. H. Liang et al. tackled the multiobjective combined dispatch by developing a hybrid and improved version of bat algorithm [12] and implemented on large scale systems considering power flow constraints. The conducted dispatch was static based on conventional energy resources. B. Lokeshgupta et al. proposed a combined model of multiobjective dynamic economic and emission dispatch (MODEED) and demand side management (DSM) technique using multiobjective particle swarm optimization (MOPSO) algorithm and validated their results via three different cases studied on a six unit test system [13] and can be extended towards distributed generation in microgrids.

In reported literature [14-16], in most cases, only one technique has been used to solve CEED on IEEE test cases, and their results have been compared with previous work. In Table 2-1, the survey of [17] is summarized to conclude that GA is better for low-power systems while PSO outperforms in the case of high-power systems. However, what happens when these two leading metaheuristic techniques are employed together to the same system? This work deals with this novel idea, hence, both PSO and GA will be implemented individually on CEED of an independent power plant (IPP) situated in Pakistan considering all gases (NO_X, CO_X, and SO_X) for various load demands. The results will be of great importance as the data of an actual IPP will be utilized and they will also grade the performance of PSO and GA for CEED of an IPP.

In order to validate the results, a conventional IEEE 30 bus system is also considered. This work will contribute the results of combined dispatch of fuel and gas emissions (economic and environmental aspects, respectively) carried out on a power plant with two leading algorithms (PSO and GA) using MATLAB and then comparing their performance in terms of better solution, convergence characteristics (3D plots), and computation time. The implementation, comparison, and convergence characteristics of PSO and GA employed for the same systems are the main contribution of this work to the field. These characteristics were compared with each other with 3D plots to analyze the better solution yielded by the two algorithms applied for CEED of the same systems in MATLAB environment.

Table 2-1. Best optimization methods employed in different systems with regard to cost, emission, and time

No.	System	Cost-effective	Emission-effective	Time-effective
1.	1 power unit, 2 cogeneration units, and 1 heat unit	Harmony search and genetic algorithm (HSGA)	X	Cuckoo search algorithm (CSA)
		Nondominated sorting genetic algorithm (NSGA-II)	Nondominated sorting genetic algorithm (NSGA-II)	Nondominated sorting genetic algorithm (NSGA-II)
2.	1 power unit, 3 cogeneration units, and 1 heat unit	HSGA	X	Gravitational search algorithm (GSA)
3.	4 thermal generators, 2 cogeneration units, and 1 heat unit	GSA	X	Effective cuckoo search algorithm (ECSA)
		Grey wolf optimization (GWO)	GWO	GWO
4.	13 power units, 6 cogeneration units, and 7 heat units	Exchange market algorithm (EMA)	X	Modified particle swarm optimization (MPSO)
5.	26 power units, 12 cogeneration units, and 10 heat units	MPSO	X	MPSO

2.2. Optimal sizing of standalone renewable energy based (PV-WT-BESS) system:

In the last two decades the production of electrical power has increased significantly due to the increase in the load demand. The world statistics indicates that in the coming years there would be a remarkable increase in the power consumption, which will require additional sources of energy. Also, the majority (more than 80%) of the current energy demand is met by means of conventional energy sources [18, 19]. These conventional sources are not only finite and fast depleting, but also a threat to our environment in many ways. Thus, here arises an urgent call for cost-efficient, reliable and environmental friendly alternating sources of energy.

At present, renewable energy sources such as wind, solar, geothermal, biomass and hydropower have received much attention for electricity generation. Currently, they are fulfilling somewhere between 15% - 20% of the world total energy demand, while in the second half of the 21st century this figure might cross 50% with right policies in place [20, 21]. However, the main problems with the use of renewable energy sources is always been reliability as these sources are often highly dependent on nature and weather conditions. For example, all climates are not suitable for solar energy and wind does not blow all the time during those periods. Hence, these energy sources cannot provide continuous power supply to the load individually. In order to solve this problem and enhance system reliability two or more generation units can be combined together in the so called hybrid system concept.

For hybrid system design optimum sizing is another important issue. While over sizing might solve the reliability problem, but it can be costly. Therefore, optimum sizing is considered by the number of system components which met the load demand with the minimization of total system cost. Hence, a great deal of research is going on in obtaining the optimum size of the hybrid system and a summary of such system can be

obtained from [22-28]. However, this hybrid system might have some minor drawbacks such as power fluctuations (due to the intermittency of the solar irradiation and wind speed) if it is not designed in an appropriate manner. But, it can be smoothened with the use of energy storage system. The storage batteries accumulate the surplus power and discharge when there is deficiency in the overall power generation. The addition of storage system also helps in avoiding the system to be oversized. In order to divert the remaining power after battery is fully charged, dump load is used and minimization of this load can lead to minimizing the cost of energy (COE) [29]. Only minority of the researchers consider surplus power in their design objective. This optimization problem has been addressed in literature using different modern techniques [30-35].

This work proposes iterative filter selection approach for the renewable energy system design. Iterative filter selection approach would be a useful tool in designing hybrid energy system in order to meet the required load demand while maximizing the system reliability and minimizing the total cost. The minimization of surplus power in the dump load would also be taken into account as one of the major objective. Different parameters such as Energy Index Reliability (EIR), Expected Energy Not Supplied (EENS) and total cost which includes initial cost, salvage value and operation and maintenance cost are also included.

2.3. Vulnerabilities and Countermeasures in Electrical Substations:

The impending and continued threat of cyberattacks on modern utility grids has called for action from the different stakeholders of the electricity sector. This calls for a thorough investigation and review of the weaknesses present in the distribution substations – the backbone of the grid – that can attract attackers to achieve their malicious objectives. The present survey deals with this issue and identifies both the common and specific vulnerabilities present in substations that can be exploited by

potential attackers. This work approaches the topic, for the first time, from an attacker's perspective, in order to categorize the possible attack vectors that could be used to first access the substation network, and then disrupt the substation operations under the purview of IEC standards. The reported literature in the field was critically analyzed from an attacker's perspective to highlight the potential threats that can become a liability in cyberattacks on substations. Countermeasures pertaining to these cyberattacks are then detailed and the main elements required for a comprehensive electrical substation cybersecurity solution are finally outlined.

The conventional power system began its journey with generation of alternating current (AC) which was widely accepted over direct current (DC) mainly due to its capacity of safely reaching longer distances with more power. The power plants utilize various sources of energy such as hydral, thermal and nuclear to convert mechanical energy into electricity through AC generators. The generated electricity is then transmitted towards the consumers through transmission lines over towers and poles. At substations, transformers step up and step down voltage levels at generation and distribution sides respectively. The distribution substations step down the voltage levels according to the requirements of different types of consumers such as industrial, commercial and residential. In order to keep the entire operation running smoothly, system operators used to communicate on telephones across generation, transmission and distribution sections of power system.

The electrical power system has now transitioned to smart grids, which include advanced technology for remote and real-time monitoring, control and protection of the grid [36]. With the advancement of technology, both the electrical equipment and communication network have evolved nowadays. The system components have shifted from telephones to computers, from copper cables to ethernet/fiber-optic cables and

from simple relays to intelligent controllers [37]. The monitoring and control is possible from remote locations in real time due to internet relying on fiber optic cables. Presently, the communication network of electric grids has enlarged in the form of transmission and distribution control centers. They monitor and control the events and actions from the substations. Moreover, there are growing awareness and continuous shift worldwide to adopt and increase reliance on clean energy. Hence, energy producers are incorporating renewable energy sources (RESs) such as solar and wind into the grid both at generation and distribution levels. As a result, the electric grid is becoming more complex (e.g., bidirectional power flows) and distributed in nature [38]. Future utilities will be even more advanced in the integration of power system with communication technology [39, 40] as shown in Figure 2-2. The communication network of electric grid today is expanding over the consumers enabling them to contribute their excess energy to the grid, from renewable installations. Moreover, the electric vehicles and energy storage devices at generation and distribution levels will be incorporated in future grids, making the grid more flexible and distributed. Both the electric vehicles and energy storage devices will be scheduled to consume energy from the grid in off peak hours and will be allowed to deliver energy to the grid in peak hours. This remote real-time monitoring and control is beneficial for the system operators in control centers, and to accommodate evolving and distributed technology. However, such advanced communication networks also increase the attack surface and could be exploited by hackers with malicious intent. While smart grids greatly improve the efficiency and operations of electrical distribution, they are also prone to cyberattacks and other new challenges [41, 42]. To cope with such challenges and issues related to the cyber security of smart grids, new standards have been developed to achieve safe grids with secure communications [43-45]. We therefore believe that it is important to

simultaneously study the current and future standards, the cyberattacks methodology and the existing countermeasures in order to develop a cybersecurity solution compatible with the evolving electrical substations in the smart grids.

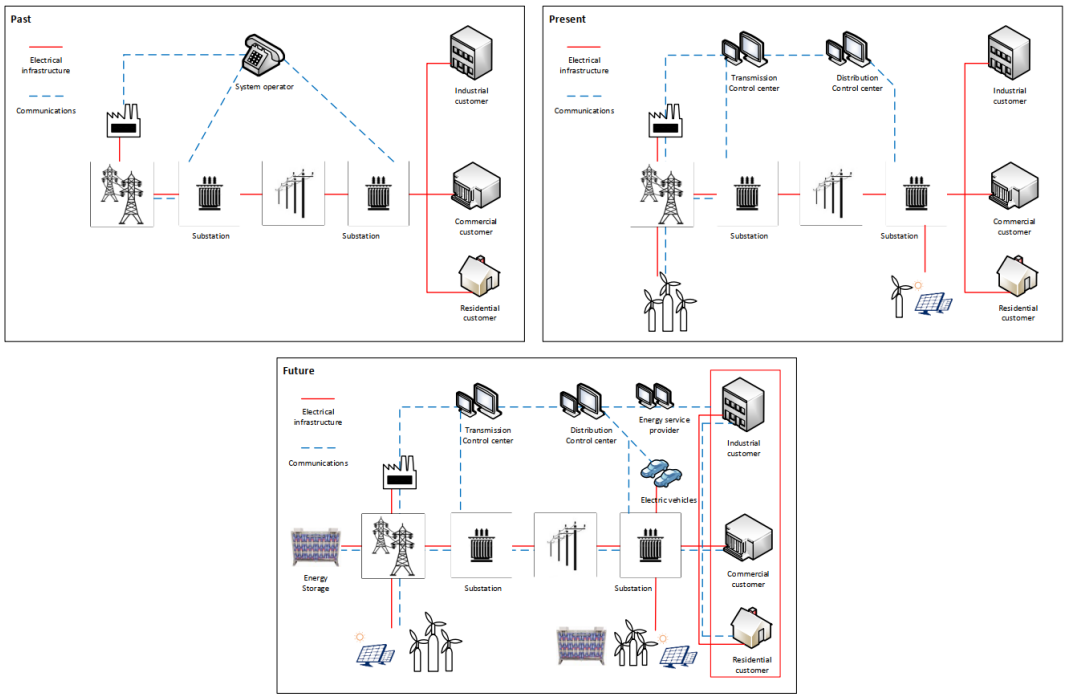


Figure 2-2. Evolution of power grids [46]

The literature already features several surveys and position papers on smart grids cybersecurity [43, 46-49] that have been considered. The literature also includes vulnerability analyses, various attacks on network and data with their modeling, detection of these attacks and their mitigation methods [50-54]. Researchers have even analyzed the standards related to smart grids and cybersecurity and identified the gaps in them [44, 45, 55]. The standards associated with power system involves both the legacy and recent standards such as IEC-101/104 and IEC-61850 respectively [12, 29]. In modern smart grids, especially with the integration of renewables, IEC-61850 has been widely adopted as de facto standard and it is continuously evolving. The standard was originally developed for interoperability and automation inside a substation but has now extended its scope to microgrids with distributed generation. The protocols

involved in any standard are initially designed exclusively for communication purposes, without security in mind. Due to this reason, there is a huge amount of work in present literature on cybersecurity of smart grids in general [56-59]. However, a thorough investigation of vulnerabilities targeting modern electrical substations based on IEC-61850 automation protocols is seldom addressed. This work has insightful contribution in this direction and apart from background and evolution of electrical substations, its novelty can be summarized by the following points:

1) Our survey discusses in detail the vulnerabilities, exploitations, cyberattacks and countermeasures with focus on electrical substations evolving with ICT.
2) Our analysis further classifies the methodology, scenarios and impact of cyberattacks in the substation domain according to a security taxonomy. This helps in identifying gaps in current research that will be addressed in future work.

In order to design an efficient cyber security solution for electrical substations, the vulnerabilities that can represent a potential cybersecurity threat have first to be identified and categorized. The main contribution of this work is an analysis of electrical distribution substation architecture, in particular from the perspective of cyber security, in order to frame the attack surface, and identify vulnerabilities that could be exploited by an attacker through accessing and remotely disrupting the operations of such substations.

2.3.1. Background

Electrical substations

Electrical distribution substations are the building blocks of the grid distribution system. Given the vast volume of substations, and their geographical dispersion, remote operations have become a must for efficient operations. Market research studies [60-

62] have indicated that distribution automation (DA) and advanced metering infrastructure (AMI) are currently the two smart grid technologies most adopted by utility companies.

Distribution substations are composed of devices that may come from multiple vendors and can communicate via Ethernet switches on the local area network (LAN) in a interoperable way, if they implement international standards, such as the International Electrotechnical Commission (IEC) standard 61850 [47]. The main difference between conventional and digital substations is the process bus. "A process bus system is a remote I/O architecture for protection, control, monitoring and metering allowing designing out copper wiring in substation switchyards and replacing it with standardized optical fiber based communications" [63].

Kowalik et al. demonstrated the Ethernet-based communication upon which modern substation automation systems (SASs) are based, as per standard IEC 61850 [64]. The advantages include multiple connected devices, with user interfaces, increased distance between measuring and protection devices, and matched performance to those in cases of direct connection without switch. Devices can also communicate on this network with each other, the station console or a human machine interface (HMI), and with the control center via a wide-area network (WAN) [65], as shown in Figure 2-3. This architecture for digital substations ensures interoperability and enables remote access for the monitoring and control of a substation [66]; however, as noted in [67], these communication protocols could be exploited by intruders to gain access to the substation or the control center. For example, in case of coordinated attacks, the attacker can simultaneously modify GOOSE and SV packets in substations to disrupt protection and measurement functions respectively. Based on these modified packets in substations, the operators in the control center can initiate actions triggering and

contributing to further faulty operations.

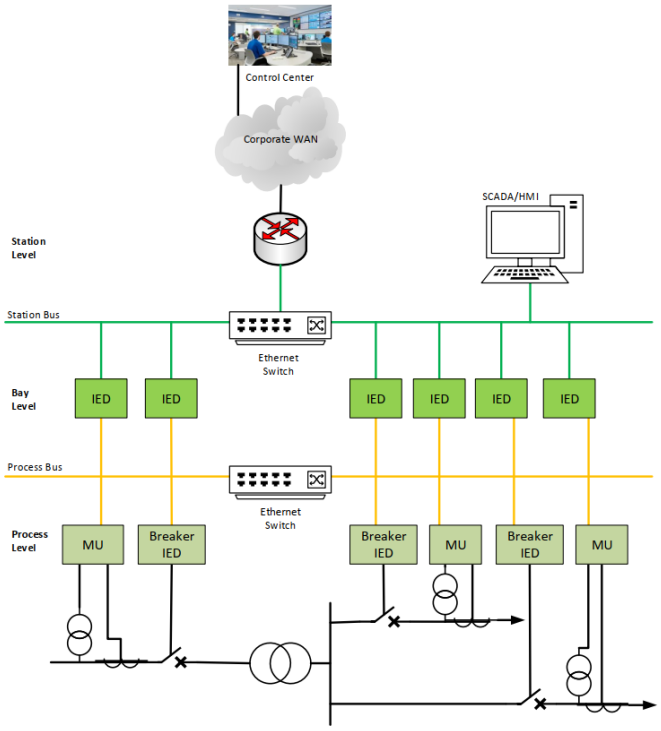


Figure 2-3. Substation automation model [47]

Cyberattacks on the energy sector

In actuality, the energy sector has been a target of increasingly sophisticated cyberattacks for the last decade [48, 68]. Blackouts cause significant inconvenience to people and the grid due to either cascaded outages (unintentional and internal) or cyberattacks (intentional and external). The risks, vulnerabilities and threats expose the system to faulty operations which damage the power system that can be both accidental (80%) and intentional (20%) [69]. The impact of such attacks has been assessed by experimental studies and test beds in laboratories worldwide [70, 71]. In 2007, the Idaho National Laboratory did a study that involved damaging the controls of a diesel generator being operated remotely [56]. Similarly in 2016, the Kaspersky Labs in Russia hosted a cybersecurity event, inviting hackers to compromise a power system simulated using a real-time digital simulator (RTDS) by accessing the data and

protective relays of an IEC 61850-based simulated power system [72].

In 2008, the Georgian electrical grid was believed to have been compromised by a Russian army cyberattack during the war between them [56]. Even in the absence of open war, cyber espionage on the energy sectors of other countries is performed undercover and can lead to cyberattacks. The first reported cyberattack on a massive scale involved a worm called Stuxnet that infected the industrial control systems of 14 sites in Iran, including an atomic plant [73]. After a year, two more worms – Duqu and Flame – were discovered in Iran. They were used for cyber espionage to gather information about their industrial control systems (ICSs). Flame has also been reported from other Middle East countries. A malware by the name of Shamoon surfaced in Aramco, Saudi Arabia's oil company, in 2012 [74]. It affected 30,000 staff computers, destroying data on the hard drives while displaying a picture of a burning American flag. The operation and production of the company remained intact, but a lot of confidential data was lost. The same malware attacked a gas-producing company – RasGas – in Qatar in the same year, affecting the staff computers and web services [75]. The damage was controlled, with no operational loss, being limited to the data on the drives. Contrary to these attacks on the information systems of energy companies, there was a large-scale direct attack on the power distribution stations of Ukraine in 2015 [76]. The attacker(s) collected information by sending phishing emails to the employees. The attack was launched by taking control of multiple HMIs simultaneously in seven substations using the BlackEnergy malware. The coordinated attack led to a power disruption that affected approximately 225,000 customers [48]. Moreover, the attackers made the communication system unavailable, disconnecting customers calling to report the problem to the call center. The software on the system was also deleted by the malware to paralyze the recovery response being attempted by the

operators. This last attack shows that cyberattacks can have a devastating effect on the energy sector due to architectural vulnerabilities resulting in an increased attack surface [77].

A typical attack in critical infrastructures which is not applicable to IT networks, is that attackers try to malfunction sensors by corrupting their measurements to generate counterfeit control commands for actuators disrupting operations in power system as shown in Figure 2-4. Furthermore, control attacks seem legitimate but have malicious packets for harmful states such as opening multiple transmission lines in power system affecting many substations and consumers. The harmful states are pre-empted using power flow analysis to neutralize such packets. The other types of attacks include monitoring-control attacks [78] simultaneously on sensors and actuators and implementation attacks targeted on embedded devices such as IEDs of electrical substations. For protection against such attacks, the first step is to model such attacks for analysis especially on active distribution networks in power grid. After modelling, the next step is to propose security assessment and framework [38, 79] to devise robust cybersecurity solution.

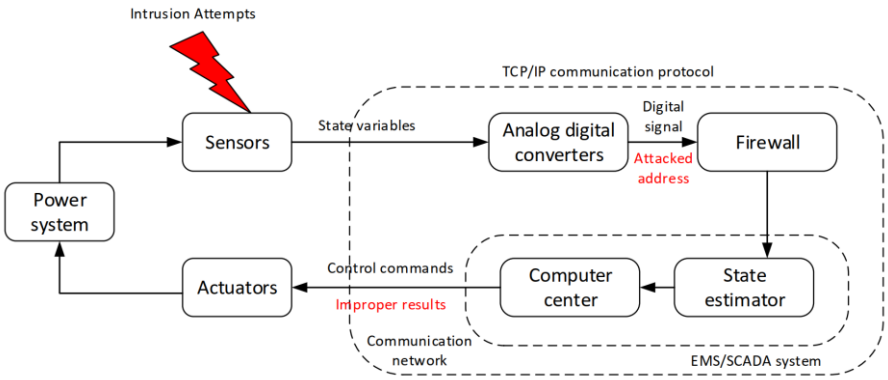


Figure 2-4. Intruder attack [79].

The points of interest for the attackers are the intelligent controllers communicating over LAN. At distributed renewable energy sources (DRESs), generation data is sent

periodically to an external server through a local controller with IP interface. The authors of [80] have analyzed the network flow and generation data for a local wind turbine installed in a university. They have noticed that although the generation data is gathered every minute, it is sent to the external server every hour only in one burst. They observed a number of unauthorized access requests from malicious IP addresses by Mirai-like botnets originating from Autonomous Systems scattered geographically. They found that both the periodic transfer of generation data and malicious attempts happen for short span of time. Moreover, they discovered that malicious scans were conducted mostly over TCP or UDP unless the attackers were focused, in which case they use crafted ICMP packets over threshold of 1500 bytes known as "ping of death". These attempts and access requests were observed on daily basis, to obtain confidential data of the wind turbine and can be exploited to attack remotely in future.

Philosophy behind development of countermeasures

The analysis of attackers methodology invites for a comprehensive cybersecurity solution for electrical substation that covers [49]:

i. Network security
ii. Data security
iii. Devices security

The substation network is analogous to territorial boundary of a country. The stronger it is, the less the chances of successful attack from outside. As this is the first line of defense, majority of the resources (70-80%) should be allocated to its hardening. If it gets breached, the substation communication and devices cannot be relied upon anymore and isolation or damage control should be prioritized. Data and devices security is also important as in-depth defense in case the perimeter is breached. However the challenge there is that devices implementing control and supervisory

commands are time critical with limited processing capabilities.

Different SASs have been developed by the leading power companies. Presently, their products have built-in security features, such as advanced user account management, detailed log files, hardened network services, advanced firewalls, intrusion detection or prevention systems, and virtual private network (VPN) technology. Their published white papers [69, 81] have provided an insight into industry practices in electrical substations, and mostly discuss the objectives of cyber security (confidentiality, integrity and availability), the five levels of security (preventive, network design, active, detective and corrective) and an in-depth defense model. Cyber security requires vigilance against both accidental and intentional threats, and network segmentation is a common approach to fulfil this requirement. Indeed, segmentation of a large network into smaller virtual LANs (VLANs), with limited access points and multiple layers of security protocols (in-depth defense model), ensures limited damage, which can be efficiently controlled.

2.3.2. Evolution of electrical substations

Traditional substations

A substation is a node in a power system that connects transmission and distribution lines by switching equipment and transformers. The monitoring and control equipment, such as current transformers (CTs), voltage transformers (VTs), phasor measurement units (PMUs), circuit breakers (CBs), is usually housed indoors in switchgears [47]. The interconnection of these devices used to go through parallel copper wires in the 1980s, but evolved through communication protocols such as Modbus, the distributed network protocol (DNP3) and the inter-range instrumentation group (IRIG-B). Modbus was designed for industrial control systems, whilst DNP3 was intended for the electricity network and IRIG-B was designed for time-synchronization without a

network [49]. These legacy protocols were designed solely for connectivity between devices, with no considerations for cyber security. They are being secured nowadays for existing installations as an additional layer. The monitoring, control and protection of an electrical power grid is carried out by centralized supervisory control and data acquisition (SCADA) systems [51]. This works on the master/slave paradigm through the master terminal unit (MTU) in the control center, and through locally distributed remote terminal units (RTUs) in the substations. These RTUs collect the local data and control switchgear equipment and interact with the MTU in the control center [47, 66]. The SCADA system finds application in various sectors, such as water, oil and gas, and power.

The traditional substation consists of an RTU or programmable logic controller (PLC), which is hardwired with copper cables to the sensors, in order to relay information back to the control center, as shown in Figure 2-5. Traditional protocols for DA include Modbus, DNP3 protocols [82] and/or IEC 60870-5-101/104 or other proprietary protocols. These substations in a power grid are monitored and controlled by a SCADA system, while SAS is used specifically for digital substations.

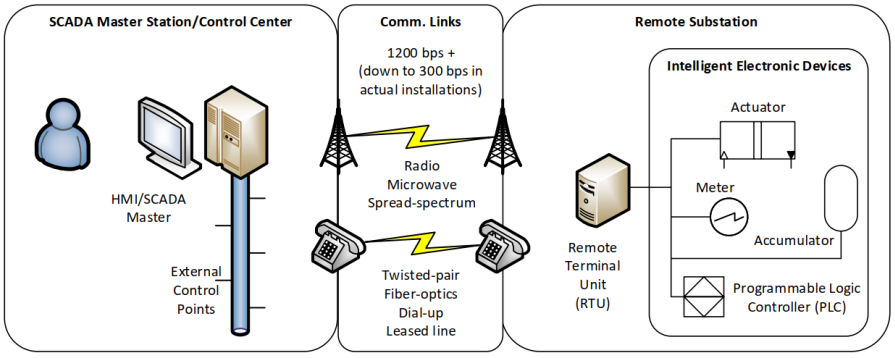


Figure 2-5. Schematic of traditional substation [83]

Digital substations

Digital substations are composed of a myriad of equipment, such as switchgears, measuring equipment (CTs and VTs), CBs, capacitor banks, transformers or microprocessor-based units, called intelligent electronic devices (IEDs) [84]. IEDs are microprocessors dedicated to the protection, control and monitoring of substation equipment. The devices in a digital substation can be demarcated into three levels – station, bay and process – that are connected by two buses – station and process [47, 66], as illustrated in Figure 2-6.

- The station bus connects clock synchronization devices with global positioning systems (GPSs), as well as giving local and remote access to the multipurpose IEDs via HMI and WAN, respectively.
- The process bus connects the substation IEDs to the field devices' IEDs.
- Monitoring equipment includes current, voltage and phasor (power flow amount and direction based on magnitude and angle of voltage, current and frequency) measurements from field devices, performed by CTs, VTs and PMUs with GPS, respectively. These analog measurements are transferred to MUs for sending to IEDs after digital conversion, merging and sampling with time stamps [82].

- The protection and operation devices in substations are CBs, disconnect switches, voltage regulators and capacitor banks, which are controlled by IEDs based on the data received from MUs. In the case of faults or abnormal conditions, the IEDs send tripping signals that isolate the faulty portion of the substation for maintenance and limit its detrimental effect.

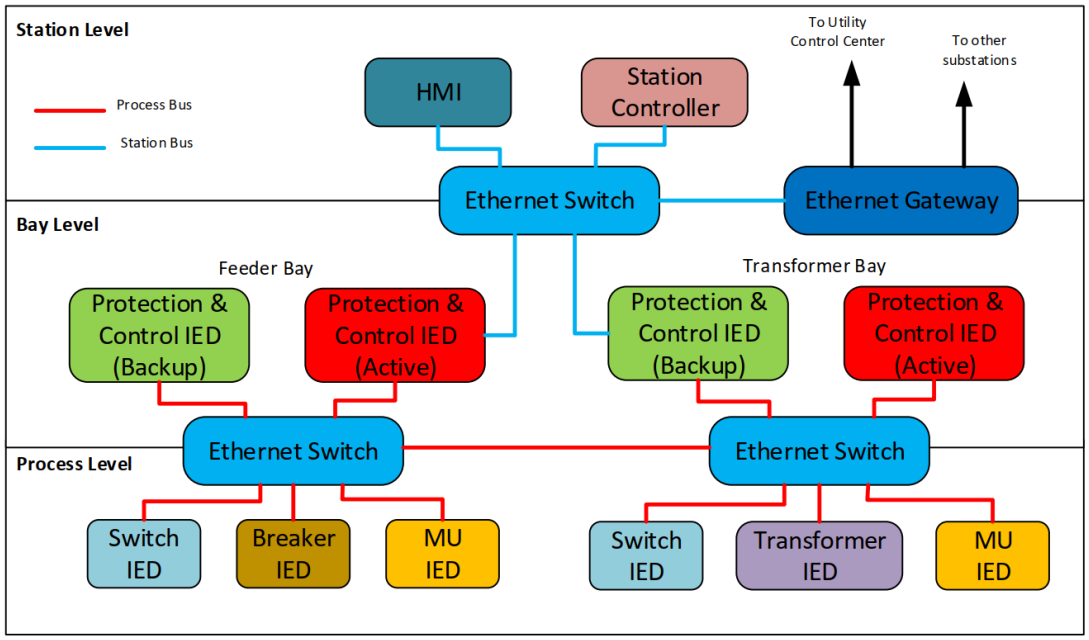


Figure 2-6. Substation automation model [57]

In new installations, substations in the power industry are being deployed based on SASs, according to the IEC 61850 standard. In digital substations, hardwiring has been replaced by communication cables and fiber-optics, interconnected through switches and routers to form a LAN. Devices are connected to the LAN (as shown in blue in Figure 2-7), and information is exchanged among them and with the control center, using the following protocols and messages, as defined by the IEC 61850 standard [85, 86]:

1. Generic Object-Oriented Substation Events (GOOSEs) for tripping signals from IEDs to CBs;

2. Sampled Measured Values (SMVs) for measurement values from merging units (MUs) to IEDs;
3. Manufacturing Message Specifications (MMSs) for the exchange of measurement readings and control commands between HMIs and IEDs; and
4. Simple Network Time Protocols (SNTPs) for time synchronization of IEDs with respect to the GPS master clock.

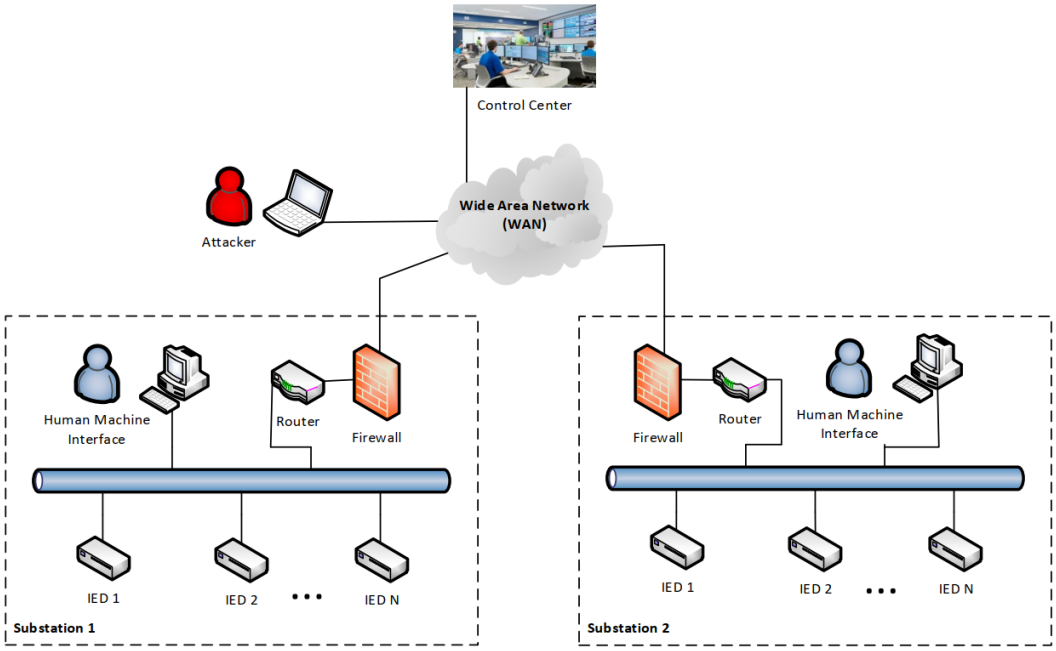


Figure 2-7. Schematic of digital substation [84]

Substation automation standards

Digital substations are automated through IEDs that report to the control center via a gateway. This was an intermediary development of the 1990s, where the problem was to connect different items of vendor or version equipment together to avoid costly protocol converters or reengineering [82]. In the early days, master/slave serial protocols were used for substation automation. New implementations of these protocols, adapted to Ethernet and TCP/IP, were subsequently developed. The most common included the Modbus RTU, IEC 60870-5-104 (the encapsulation of IEC

60870-5-101 over Ethernet) and DNP3 [87]. As of today, the IEEE and IEC protocols DNP3, IEC-60870 series and IEC-61850 have been adopted by most of the deployments worldwide, with the latter accepted as the new *de facto* protocol for SAS communication networks and systems. The IEC-60870-5-104 and IEC-60870-5-101 protocols were engineered with no in-built security, as well as several known vulnerabilities, such as the absence of checksums or a one-byte checksum, respectively [88]. To address these concerns, both IEC-62351 and IEC-60870-5-7 (IEC-60870-5 series security extension for secure authentication) were released to provide these protocols with at least authentication and encryption mechanisms. Recent reports have indicated that the industry is not applying these new security measures due to the complexity associated with their implementation [89, 90].

In the early 2000s, international bodies, such as the IEC and IEEE, were working on standardized communications for power utility automation to achieve interoperability among heterogeneous IEDs. This led to standards such as IEC 61850 that would ensure an open architecture and future extendibility in the substations. IEC 61850 has, since its conception, expanded its application to communications outside of substations' automation functions, and can be used to ensure the interoperability of all devices in a substation or to communicate with the control center or distributed energy resources (DERs) [91]. Table 2-2 shows the different parts the standard is divided into and is based first on the modeling of data objects (equipment of a power system), and then their mapping into communication services. This segregation feature of the standard enables interoperability among devices from different manufactures. The application of Ethernet-based communication standardized the communication services in digital substations, producing reduced engineering costs [47, 66, 82]. The devices in the substation are configured using substation configuration language (SCL) in a file

format with .SCD extension. Such files define, and provide the settings and parameters for, the substation devices, such as IP addresses, destination media access control (MAC) addresses and VLAN-ID/PRIORITY, and need to be updated to reflect any changes made in the connectivity and/or role of the devices [92]. For this reason, they are a valuable target for attackers, who can perform modifications to substation IED behaviors to produce malicious outcomes. To access these files, attackers can either process through a compromised HMI in a substation or through remote access to the substation's network with the help of various cyberattack tools.

Table 2-2. Contents of IEC 61850 standard [47]

IEC 61850 Parts	Title	Version	Date
Part 1 (TR)	Introduction and overview	ed2.0	2013/03
Part 2 (TS)	Glossary	ed1.0	2003/03
Part 3	General requirements	ed2.0	2013/12
Part 4	System and project management	ed2.0	2011/04
Part 5	Communication requirements for functions and device models	ed2.0	2013/01
Part 6	Configuration description language for communication in electrical substations related to IEDs	ed2.0	2009/12
Part 7-1	Basic communication structure – Principles and models	ed2.0	2011/07
Part 7-2	Basic communication structure – Abstract communication service interface (ACSI)	ed2.0	2010/08
Part 7-3	Basic communication structure – Common Data Classes	ed2.0	2010/12
Part 7-4	Basic communication structure – Compatible logical node classes and data classes	ed2.0	2010/03
Part 7-410	Basic communication structure – Hydroelectric power plants – Communication for monitoring and control	ed2.0	2012/10
Part 7-420	Basic communication structure – Distributed energy resources logical nodes	ed1.0	2009/03
Part 7-510 (TR)	Basic communication structure – Hydroelectric power plants – Modelling concepts and guidelines	ed1.0	2012/03
Part 8-1	Specific communication service mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3	ed2.0	2011/06
Part 9-2	Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3	ed2.0	2011/09
Part 10	Conformance testing	ed2.0	2012/12
Part 80-1 (TR)	Guideline to exchanging information from a CDC-based data model using IEC 60870-5-104	ed1.0	2008/12

IEC 61850 Parts	Title	Version	Date
Part 90-1 (TR)	Use of IEC 61850 for the communication between substations	ed1.0	2010/03
Part 90-4 (TR)	Networking engineering guidelines	ed1.0	2013/08
Part 90-5 (TR)	Use of IEC 61850 to transmit synchro phasor information according to IEEE C37.118	ed1.0	2012/05
Part 90-7 (TR)	Object models for power converters in distributed energy resources (DER) systems	ed1.0	2013/02

The communication models in the standard are based on the client/server and publisher/subscriber philosophy. Client/service communication is done through GOOSE and multicast SV messages, while most communication is based on the client/server method via MMS messages [47]. GOOSE and SV are time-critical messages (less than 3 ms), and are directly connected to the Ethernet data link, bypassing the above-communication layers used in MMS messages, as illustrated in Figure 2-8. GOOSE is the most intercepted and targeted message by cyber attackers because it has an immediate effect, as it sends tripping signals to the CBs from the IEDs in the case of a fault. Hence, the intent is to alter this message to generate false protection signals that disconnect electricity services. Other messages (i.e. SVs) are used to send sampled current and voltage measurements (from instrument transformer CTs and VTs, respectively), which are gathered by MUs, and then forwarded to IEDs for appropriate action. Such messages constitute power-state estimations that constitute the eyes of the operators for decision-making. An attacker can obtain confidential information from such messages, and can then formulate an action plan, by either observing, or smartly modifying, these messages to achieve the objective.

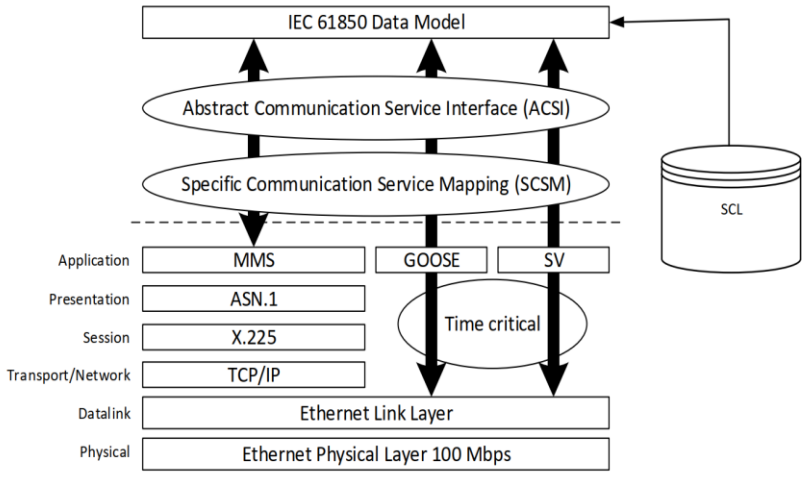


Figure 2-8. Model showing IEC 61850 communication layers [47]

The present electrical substations contain distributed renewable energy sources (DRESs) being recently adopted and have integration and intermittency issues. The associated standards are also not much developed yet and hence the attackers can exploit the integration sites much easily as weak spots to hook into the communication network of smart grids [80]. In [55], the authors have conducted a short survey on these standards addressing gaps and provided suggestions for further improvement. The international standard IEEE 1547-2018 and European standards CLC/TS 50549 and EVS 50438:2013 deals with the integration of DRESs to the electric grid. They pointed out the communication deficiencies at generation, transmission and distribution sides that can become security challenge aiding the attackers in their favour. They suggested providing guidelines for the missing communication links in order to standardize them and making them robust for any external breach. As mentioned above, efforts to secure these protocols are addressed by the industry standard IEC 62351 “Power systems management and associated information exchange – Data and communications security” [93]. IEC 62351 provides authentication and encryption mechanisms for TCP/IP-based protocols. Figure 2-9 represents the IEC mapping of each protocol and its interaction with the different components of a smart grid, including substations.

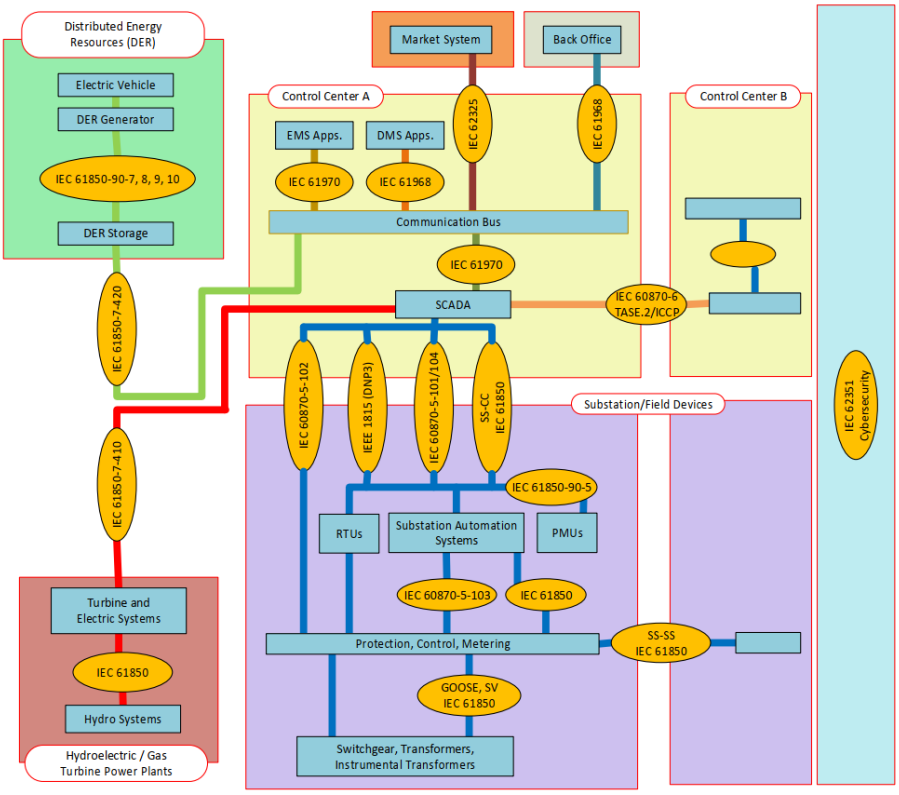


Figure 2-9. Architecture of IEC TC57 communication standards [93]

2.3.3. Cyber security concerns in the energy sector

In this section, the main cyber security issues and security requirements in the energy sector are discussed. Then the general methodology used by cyber attackers to launch sophisticated and targeted attacks are explained.

Vulnerability analysis and security requirements

According to a vulnerability analysis conducted by the Industrial Control Systems – Cyber Emergency Response Team (ICS-CERT) in 2013 [69], authentication flaws were the most common type of vulnerability, followed by factory hard-coded credentials and weak authentication keys. According to the same report for 2015, there were 46 attacks reported, mostly to the information technology (IT) systems of the energy sector [94]. The three mandatory security requirements to secure a network are availability, integrity and confidentiality [69]. Availability is to have complete control and access to

the system whenever it is required, as the operators are in complete darkness otherwise. Integrity is the ability to shield the information from malicious or even unintentional modification. Confidentiality is to make sure there is no disclosure of unauthorized information. If, in a network, these three main security features are implemented with the appropriate trade-offs relative to the constraints of the system under consideration (e.g. security vs. performance, as explained in the next paragraph), then it is considered to be a robust system for countering cyberattacks.

The preferred order of the security requirements depends on the context. In power systems, availability is of the utmost concern, followed by integrity and confidentiality, in contrast to IT networks, where confidentiality comes first, followed by integrity and availability [49]. Moreover, some voices in the industry have suggested that integrity should replace availability as the main goal in ICSs [95]. The rationale behind this claim is based on the fact that security in ICSs cannot be guaranteed without integrity, and therefore ensuring the continuity of operations without controlling the parameters of supply might defeat the purpose altogether. For the particular case of the electricity sector, the analogy is quite straightforward; providing electricity with no control on the quality variables represents a potential risk for the consumers, electrical crew and the infrastructure itself. This preferential list serves as a guideline for devising a defence model that keeps the severity and likelihood of a particular cyberattack under consideration. It is also important to understand the attacker's goals and mode of operations in order to best mitigate the threats. During the security analysis of electrical substations, a vulnerability assessment is performed to detect existing vulnerabilities and a corresponding probability of attack(s) is computed. This probability can be calculated by factoring in potential attackers' budget, capability, motivation and undetectability [96]. They are scored depending on their level from very low to very

high corresponding to 0.1 and 1 respectively. On the other hand, the vulnerability of assets are also scored by methods such as Common Vulnerability Scoring System (CVSS) which rank the asset vulnerabilities on a scale of 1 to 10 and is further normalized to 0-1 scale for consistency. Finally, the probabilities of both occurrence and severity of attack are computed by accounting all these factors. The probability can be modelled by a Poisson distribution [97]. Markov decision process is also used to define optimal policies by implementing attack and defense model [97].

Taxonomy of cyberattacks for electrical substations

Before describing the actual attacks, the taxonomy being used needs to be described. In the context of cybersecurity, taxonomy consists in grouping and classifying categories that describe the nature and impact of incident (attack) as described in [98] by European Network and Information Security Agency (ENISA) and other group members. Different taxonomies have been developed and presented in the Industrial Control System Security field [98-101] into models such as the Attack-Vulnerability-Damage (AVD) [100] and the Threat-Attack-Vulnerability-Impact (TAVI) [101] models. These models describe the vulnerabilities exploited and damage or impact caused by different attacks in a formal way to enable a systematic work for security analysts. They can then be used to study the dynamics of the attacks with better visibility and create the countermeasures in the process. The AVD model in particular has been widely used in the community and even extended by subsequent researchers (such as in TAVI), hence this model is adopted in our survey to classify the cyberattacks in addition to countermeasures relevant to electrical substations. The AVD model consists of three components:

- The first component i.e. **attack** consists of the origin (local or remote), the actual action that is performed and the target of the attack (network, process, system, data or users).
- The second component i.e. **vulnerability** describes the weakness that can be exploited and it could be a configuration issue, a design issue or an implementation one.
- The final component i.e. **damage** describes the effects on security state (on confidentiality, integrity or availability), on task performance (timeliness, precision or accuracy) and severity level which qualitatively measures the level of the impact (low, medium or high).

The comprehensive AVD model is summarized in Figure 2-10 and this taxonomy will be used in the rest of this survey and adapt it to present the methodology used by cyber attackers in order to disrupt normal operations of an electrical substation.

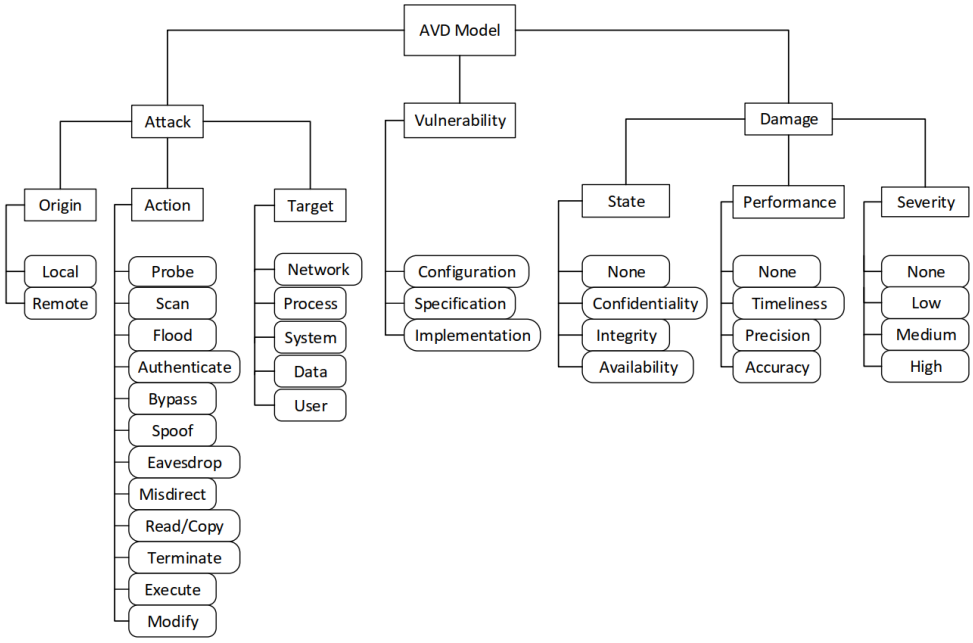


Figure 2-10. Comprehensive Attack-Vulnerability-Damage (AVD) model

Cyberattack methodology

Targeted cyberattacks are focused here because they are more sophisticated and have a

higher success rate. Intended cyberattacks are carried out in a well-planned manner. There are four stages in which professional adversaries operate in order to execute a successful cyberattack – reconnaissance, scanning, exploitation and maintaining access [49].

- The reconnaissance phase consists in observing and analyzing the network to gather information on the target. Obtaining valuable information from insiders, both smartly or fraudulently, is also part of this stage, and is termed ‘social engineering’.
- Then comes the scanning of IP addresses, ports and services of the network, during which the attacker looks for vulnerabilities to be exploited for the cyberattack. The legacy protocols Modbus and DNP3 are the most affected by such scanning attacks.
- Exploitation is the core of the attack, during which the adversary actively interrupts the network either by installing malware (viruses, worms, Trojan horses, etc.) or corrupting the communication at the individual or collateral level.
- Finally, attackers want to maintain access to the target by redeeming secret backdoor and malware programs invested in earlier to maintain their access on a substation network.

Attacks on power utilities can be further subdivided into three main categories – physical, cyber and human – that depend on the dominant attack vector. This is shown in Figure 2-11, with subcategories [102].

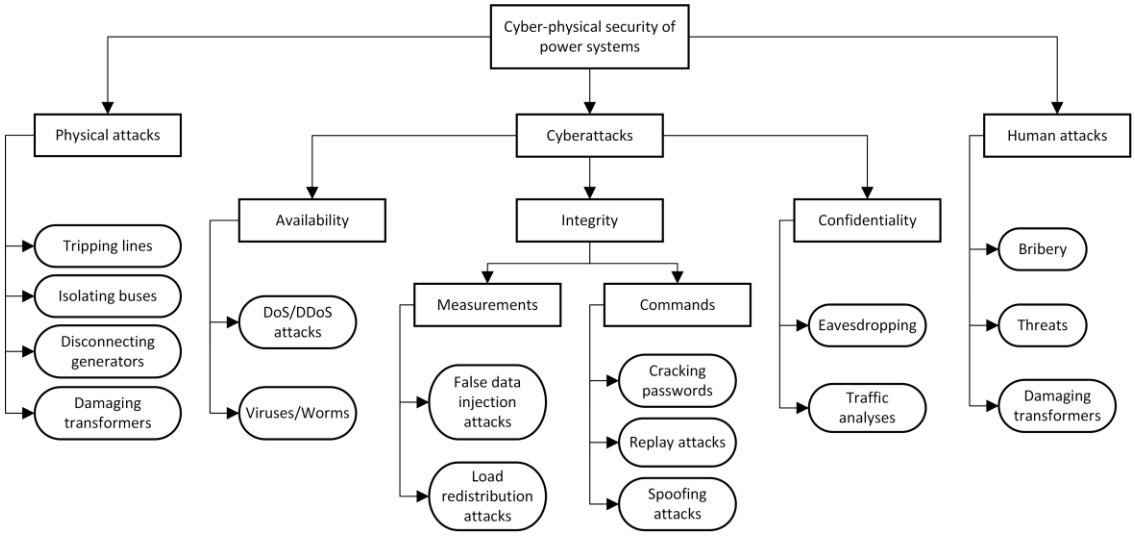


Figure 2-11. Schematic showing different potential attacks on a power grid [102]

Physical attacks refer to the damage and/or actions, by force, caused accidently or maliciously to power equipment by the public, personnel or environment. For example, a tree falling on a transmission line, a lightning strike on a transmission tower or isolating equipment for maintenance purposes. All of these result in the disruption of services to consumers, and such events can be utilized by cyber attackers as weak links for propagating the damage further into the system. Cyberattacks mainly refer to attacks resulting from the remote exploitation of the network at the software level, which requires detailed information about the system, which is obtained by self-learning and/or social engineering of human personnel either working or associated with the power industry. Social engineering of humans can involve various methods for stealing information, ranging from abusing human trust to exploiting personal relationships, through threats and bribery.

Note that these categories are not mutually exclusive, but can be combined for the different stages of a sophisticated attack. For instance, human attacks, such as social engineering, are often used in the reconnaissance phase, while cyberattacks are the prime vector for the remote exploitation of vulnerabilities. While physical attacks can have devastating impacts, they also require the attacker to physically go to the target

location, thus risking exposure. They are thus potentially much more hazardous than cyberattacks. With the advent of the smart grid and DA, there are increased opportunities for attackers to connect to the network and perform attacks remotely, minimizing their risk. There are actually various network attacks that can be launched in the exploitation stage of a cyberattack, either in isolation or in a group, to fulfil the desired agenda [47, 49, 82, 84]. Some of the more well-known types of attacks are discussed here, with brief descriptions.

- **Malware:** This includes viruses, worms and Trojan horses, the aim of which is to infect a device or system in a malicious way and help the attacker to steal information for either cyber espionage purposes or to impact the intended system. Practical examples of such malware are Stuxnet, Shamoon, BlackEnergy, Duku, Flame and Gauss.
- **Denial of service (DoS):** The attacker bombards the target system with multiple frivolous requests, forcing it to crash and compromising availability. Hence, the system becomes unresponsive to the restoration actions initiated by the operators in the control center.
- **Man in the middle (MITM):** In this type of attack, the outsider intercepts a communication passively, prior to the action, by placing themselves in the middle of two legitimate devices. Once inside the network, they can alter the communication messages or corrupt the devices, placing the confidentiality and integrity of the system at stake. For instance, the software Wireshark Network Protocol Analyser can be used as a sniffing tool to switch communications by accessing redundant ports connected to the user interface [64].
- **Replaying:** In such attacks, the communication packets are modified and replayed to the intended receiver, challenging the integrity of the system.

Critical devices, such as IEDs, PLCs and AMIs, start behaving in accordance with the wrong data being fed to them.

- **Channel jamming:** The target of this attack is to disrupt the wireless services of the substation by sending same-frequency signals to occupy the channel. As a result, the genuine services are blocked during the period of the attack, affecting the availability of the system.
- **Popping the HMI:** The motivation of the attacker is to get remote access to the consoles in the substation or the control center. This is done by installing decoy shells to monitor and control the system and by studying the open source vulnerabilities of the operating system (OS) installed in the devices. For example, open-source tools, such as Metasploit and Meterpreter, can be used to gain administrative access to the user interface [49].
- **False data injection (FDI):** Such attacks inject erroneous data in order to corrupt the devices, especially those dedicated to measurements. Hence, the cyber attacker can generate commands based on the bad data, and the system can be deviated from its normal operation. The integrity of the system is compromised in such attacks [103].
- **Spoofing:** The attacker impersonates an authorized user by altering the address of the data packets in order to perform harmful actions in the system.

After having discussed the general methods of cyberattacks in the energy sector, the vulnerabilities and attack vectors that specifically apply to distribution substations are now focused in more detail.

Attack scenarios and impact on electrical substations

The hackers can actually attack the electrical substations by accessing system remotely from enterprise network or locally from control network [67] as shown in Figure 2-12.

In first scenario, the direction of attack is from enterprise network, to access critical infrastructure (power generators) via CSS. The impact that attacker can cause is directly related to his knowledge of the environment. The direction of attack in second scenario is from control network to attack the system (RTUs in SCADA network) through CSS under duress or for other reasons. Third direction of attack is from malware in flash drives being used to update software of different control devices such as IEDs inside different substations. The person trying to attack the system can be unauthorized or authorized user and different approaches are adopted for both kinds. The unauthorized users having limited knowledge can be directed towards emulated devices to be tracked and neutralized in the process. For the authorized users conducting attacks intentionally, alerts can be generated via isolated control paths to security system. The threats generated unknowingly from authorized users can be prevented by appropriate actions from the control network.

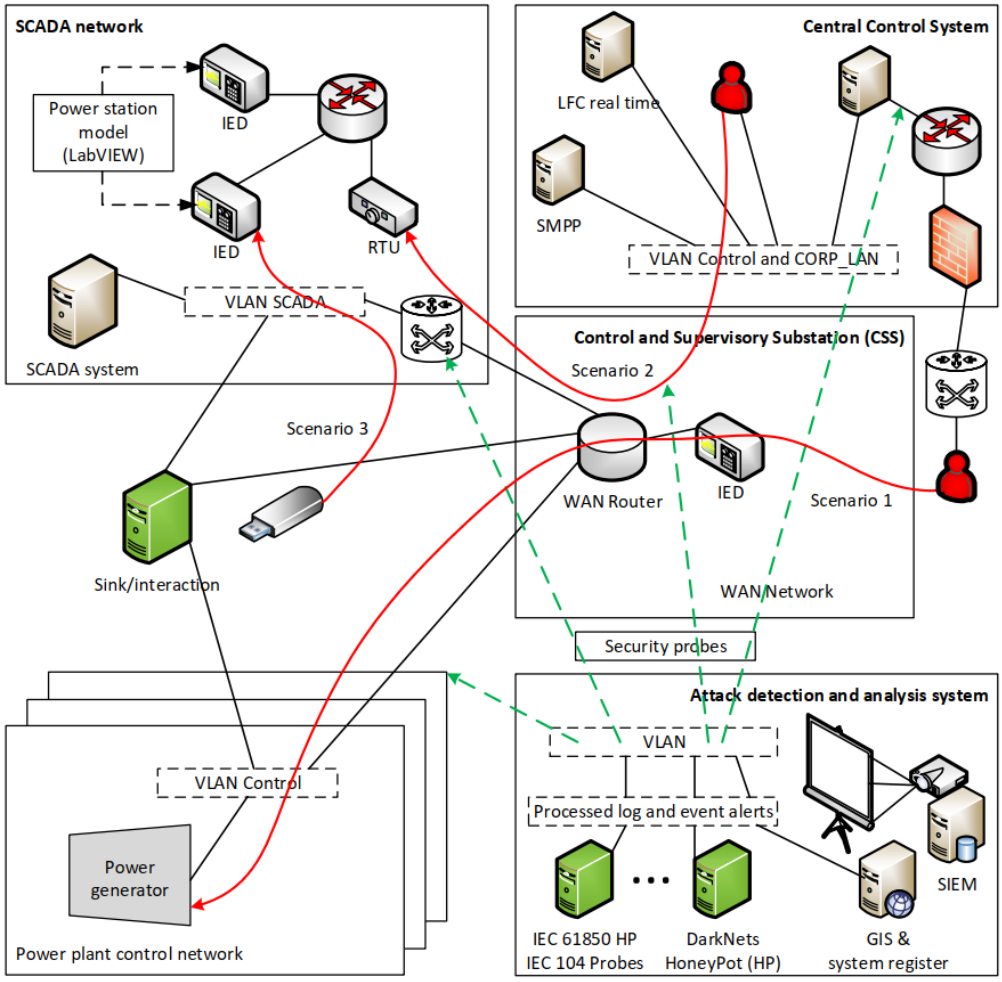


Figure 2-12. Attack scenarios [67].

The impact of attacks can be disastrous depending upon the sites of attacks (critical paths). In modern substations' communications as shown in Figure 2-13, attackers can compromise relay settings to overload transformer by tripping breakers to isolate the secondary transformer as shown in Figure 2-14 [104]. Circuit breakers CB-3 and CB-4 are tripped by the attack de-energizing transformer Xfmr 2 from the system putting extra load on Xfmr 1. In such cases, the attack trips the secondary equipment shifting its share to the primary device contributing to its physical failure or vice versa. The impact increases as attacks starts from device level towards the whole substation. Disruptive switching of isolators and breakers can also be executed with administrative privileges to trigger partial outage in a substation affecting few consumers. Moreover,

entire outage of the substation can also be targeted by opening the main incomer circuit breaker as shown in Figure 2-15. By tripping incomer circuit breaker CB-6, the incoming supply of the whole substation is cut off. This sheds load of all the consumers connected to the substation unless they are being fed by alternative path of ring network.

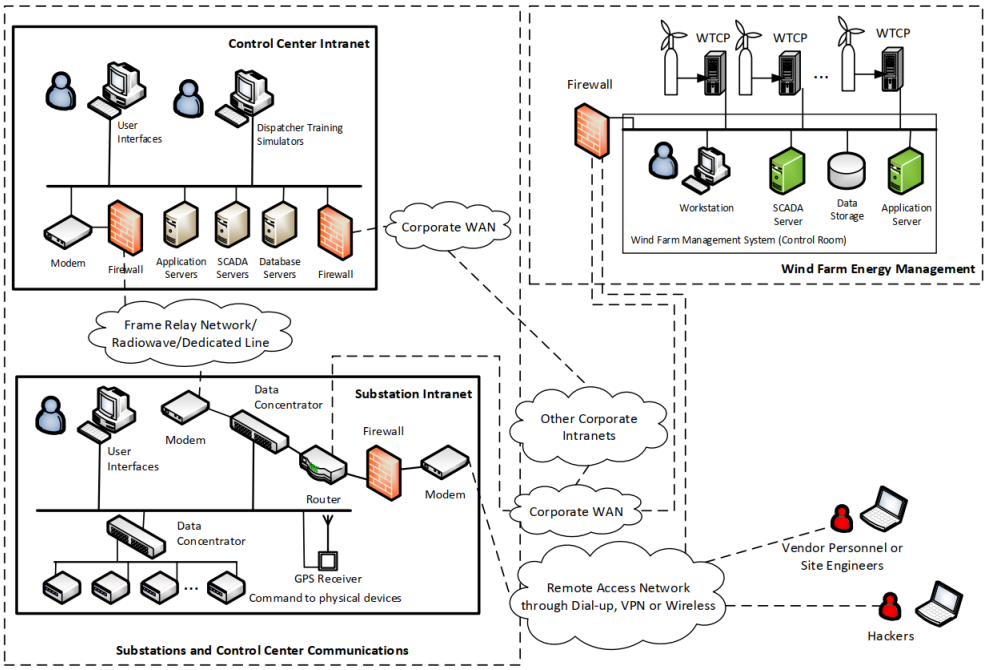


Figure 2-13. SCADA infrastructure [104].

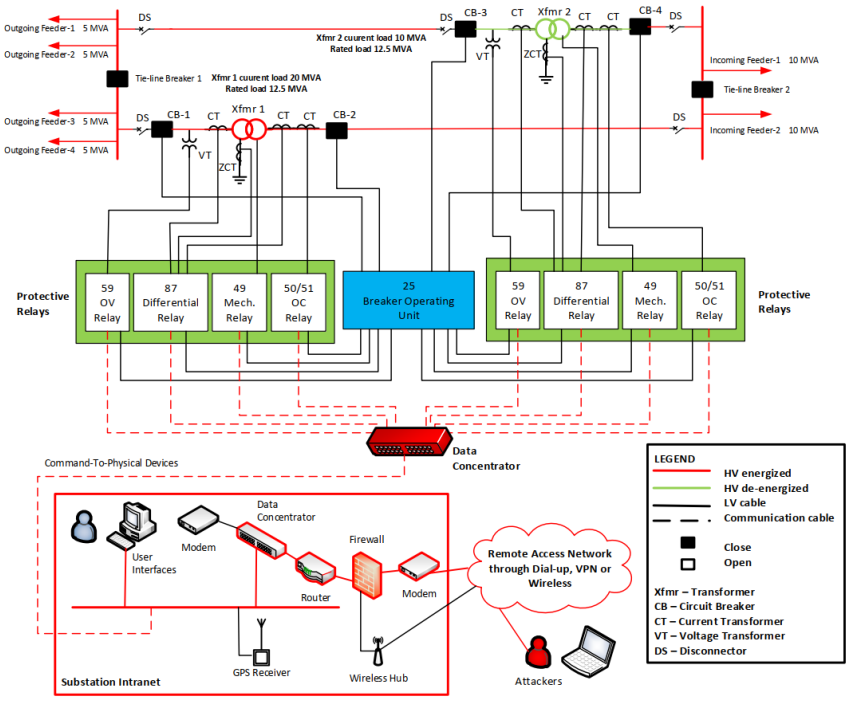


Figure 2-14. Transformer 1 overloading [104].

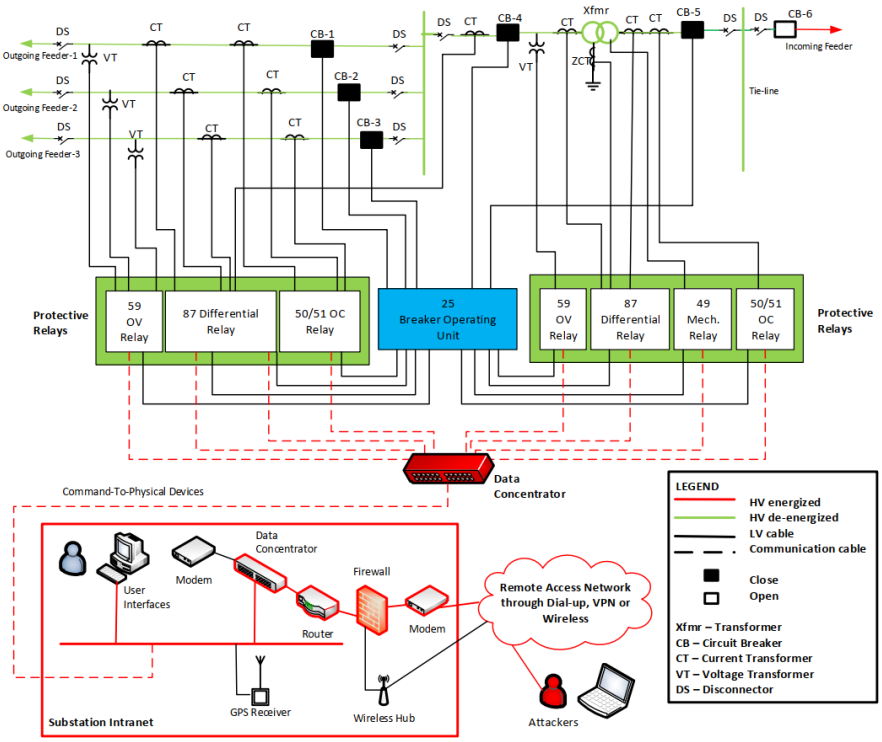


Figure 2-15. Substation outage [104].

2.3.4. Cyberattacks on electrical substations

In the case of electrical substations, the attackers mainly target the control of the relays in the substation in order to disrupt their normal operation and affect the consumers. This requires knowledge of the telecommunication single-line diagram (SLD) in order to tamper with the network protocols in a targeted way. The attacker can also hack the HMI through malware, or even attempt to take over the control center to magnify the attack level. Depending on the defense mechanism of the substation, the attacker can also trip CBs, branches, generators, loads, inject false data for power-state estimations, exploit the metering system and even compromise flexible alternating current transmission system (FACTSs) devices in transmission substations [84]. This is done by modifying the communication packets from/to IEDs, and/or the configuration of devices by modifying SCL files. This situation, if not handled in due time, can lead to cascading system failures or even blackouts, in the case of coordinated attacks. Such

attacks are launched in narrow time gaps, making it difficult for the operators to initiate a recovery mechanism.

The aforementioned four stages of sophisticated attacks on substations can be grouped into two steps:

1) Devising a method to break into the substation network;

2) Exploiting vulnerabilities to take over critical components of the substation to achieve the attack goals.

The existing literature is reviewed with an attacker's eye in order to summarize the known methods of achieving each of these steps in the case of distribution substations.

Accessing a substation network

Distribution substations are spread over vast areas, from highly populated cities to remote rural locations, and are connected to the control center through a wide range of public and private network options (fiber-optic, radio/microwaves, cellular, power line communication). As shown in Figure 2-16, these interconnections create spaces via which attackers can exploit the network [82]. The intrinsic limitations of the technologies in the wired (power line communication, fiber-optic, DSL) and wireless (WPAN, WiFi, WiMAX, GSM, satellite) communications used in the power system can also be a focus for cyberattacks [46]. For example, the high losses and channel interference in power line communications, the high interference spectrum in WiFi and the high latency in satellite signals can attract an attacker to induce a cyberattack.

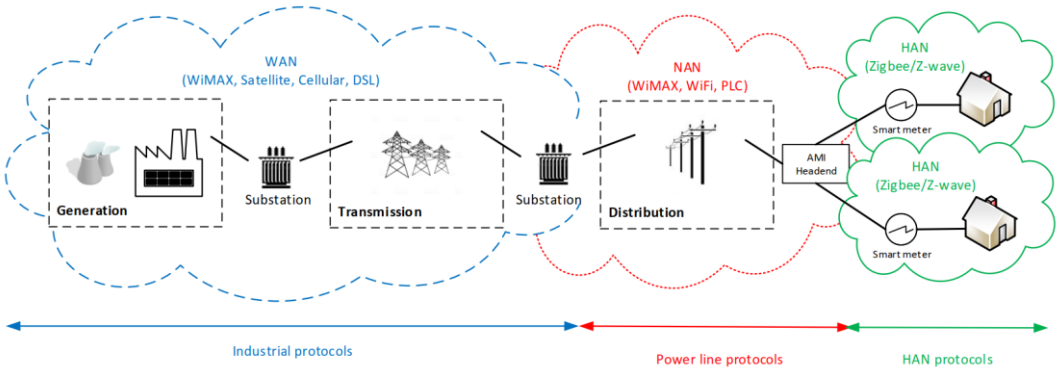


Figure 2-16. Communication network of a power system [49]

The civilian GPS bands used for the time synchronization of PMUs are mostly not secured [82]. This can become a liability, and an attacker can disrupt time-critical operations using spoofing attacks. Furthermore, it may not be feasible to monitor the huge traffic in WAN, as this will decrease system efficiency. This makes WAN more prone to cyberattacks for gaining remote access. The integration of renewable energy from the consumer end provides another access point for potential attackers. The renewables equipment is mostly consumer-owned and may not be properly configured and protected, thus posing a threat to the connected substation network.

For those cases where wireless communications are used, another set of vulnerabilities are open for an adversary to enter into the system. The common industrial, scientific and medical (ISM) band is normally used for wireless communication, which is easily accessible, and an attacker with the help of an insider could cause a detrimental effect by eavesdropping on the channel and getting access to the smart devices or station console to send and inject false data to the power equipment, which could then be operated in an undesired manner [82]. Moreover, even if the band is secured and difficult to breach, an outsider could block the substation services using jamming devices in the vicinity of the area that they want to influence. A critical attack that could be performed by an adversary would be to tamper with the time stamps of the relays

from GPS signals, leaving the operators in the control center in the blind, making them unable to execute the correct protection and recovery responses. Jamming attacks can also be used for rebooting devices to the general factory settings after an attack, making it easier to steal information. Substation consoles generally have limited computational capacity, allowing them to perform only their specified tasks. Also, the performance of the system cannot be affected by employing real-time monitoring and analysis solutions, such as an intruder detection system (IDS).

Hence, a learned and experienced attacker can gain access to a substation [84] by:

- exploiting firewalls with spoofing attacks;
- using public networks and access to the internet;
- finding weak passwords (mostly default passwords during the commissioning stage);
- exploiting vulnerabilities in old and not up-to-date OSs (old ones compatible with industrial devices, such as Win XP);
- sending infected universal serial bus (USB) flash drives to deploy malware;
- sending phishing emails to disgruntled/inexperienced personnel, or by social engineering; and
- exploiting low or faulty maintenance of vendor devices.

Exploitation after accessing the substation network

Communication messages inside a substation

Disrupting communications inside a substation is one of the prime focuses of cyber attackers, as explained above. Simply delaying messages can have a major impact because of their time criticality. In the following sections, the delay requirements in substations are outlined, and the attacks that can be performed to prevent the fulfillment of such requirements.

Delay requirements and the impact on secure protocols

There are no explicit communication requirements for message delays in the IEC-60870-5 series protocols, and there seems to be no published testing on the impact these security measures could have. Unlike DNP3 or IEC-60870-5-104, IEC-61850 is a new protocol that has taken into consideration both the cyber security and communication delay requirements. Delays are categorized by message type, and defined in the standard as shown in Table 2-3, which shows a list of the message types, their descriptions and the delay requirements in milliseconds. These restrictive constraints were taken into consideration in order to define two different scenarios [105]:

1. Non-time critical messages: TCP/IP-based TLS and MACs to ensure confidentiality and integrity.
2. Time critical messages: TCP/IP is avoided, as well as any encryption mechanism, making authentication the only protection mechanism available. For this purpose, the data-link layer is bridged directly with the application layer. Authentication is obtained with MAC using SHA, digitally signed with an RSA public key system.

Moreira et al. [47] stated that RSA signatures do not allow computations below the 3 ms required for critical messages. Similarly to the findings for IEC 60870-5-104, the available literature does not seem to cover empirical tests that evaluate the performance of each case.

Table 2-3. IEC-61850 communication delay requirements [106]

Message types	**Definitions**	**Delay requirements**
Type 1	Messages requiring immediate actions at receiving IEDs	1A: 3 ms or 10 ms; 1B: 20 ms or 100 ms
Type 2	Messages requiring medium transmission speed	100 ms

Type 3	Messages for slow speed auto-control functions	500 ms
Type 4	Continuous data streams from IEDs	3 ms or 10 ms
Type 5	Large file transfer	1000 ms (not strict)
Type 6	Time synchronization messages	No requirement
Type 7	Command messages with access control	Equivalent to Type 1 or Type 3

Delay attacks in the IEC-61850 standard

Smart substations are increasingly relying on communication networks, as per the IEC 61850 standard. Once access to a network is established, an attacker can access the HMI and IEDs by exploiting the communications between them in the form of GOOSE/SV/MMS/SNTP messages, as defined in the IEC 61850 standard. To avoid being noticed, an attacker would restrict themselves to one or a few IEDs initially, gradually taking control by sending counterfeit messages to the remaining IEDs in the substation by launching a DoS attack [53]. The attacker can also corrupt the communication inside a substation by capturing the original packets and later using delay attacks [107] such as replay and masquerade. In replay attack, the packets are not modified but are only delayed to cause faulty operations while in masquerade attack, the communication packets are both modified and delayed to achieve malicious intent [108]. In order to accomplish a successful cyberattack, an attacker is generally fully equipped with knowledge of the devices and their communications in the substation. The messages used in the substation communications, according to IEC 61850, are discussed here from the cyber attacker's perspective.

GOOSE: Multicast time-critical messages, with delays of < 3 ms, lengths of 160–310 bytes and traffic rates of up to 1.3 Mbps, are used for two-way communication between IEDs and intelligent terminals, such as CBs, for control and protection purposes in a substation, directly on an Ethernet data-link layer (non-IP traffic). Their stringent time requirements do not allow encryption, and hence they are the main targets for attackers.

An attacker can either use a MITM attack to prevent genuine tripping, by delaying the message by more than 3 ms, or can carry out false tripping of the breakers, using relay or FDI attacks, by altering the content of the message.

SV: Multicast time-critical messages, with delays of < 3 ms, lengths of 190–340 bytes and traffic rates up to 33 Mbps, are used for broadcasting the sampled values/measurements collected from field devices by MUs to IEDs in a substation, directly on an Ethernet data-link layer (non-IP traffic). Such messages are grouped with GOOSE messages from a security perspective, in terms of delay time and size. As they contain the measurement data for power-state estimations, they are prone to logical FDI attacks that keep the operator unaware of the actual performance of the field devices until the damage is done. Another crucial way is to force the operator to initiate false protection measures by feeding false data from the field devices, although this usually happens less because experienced personnel perform two-way verifications with their field crews prior to launching protection schemes.

MMS: Unicast messages, with time delays of < 100 ms, up to a length of 1480 bytes and with traffic rates of up to 1.65 Mbps, are used for two-way communications between HMIs and IEDs at the bay level to control and monitor data and documents in a substation using a network layer (TCP/IP protocol). Initially, an attacker will get hold of the active IED receiving this message using multiple attacks, such as MITM, FDI and replaying. Following this, they can initiate the DoS attack from the compromised IEDs towards the HMI, making it unresponsive to valid requests and/or commands. The potential magnitude of damage is much greater than for exploiting GOOSE/SV messages in such cases if the HMI gets into the hands of the attacker.

SNTP: Unicast/multicast messages, with time delays of < 100 ms, up to a length of 100 bytes and with traffic rates of up to 0.0001 Mbps, are used for two-way communications

between the GPS master clock and all IEDs for time synchronization in a substation using UDP. The usual attacks launched against this type of message are of the spoofing kind, altering the time information. This leads to the loss of the sequence of events because the time stamps on the IEDs for different events are made unreliable after such an attack. The substation loses synchronization, making information too vague for the operators to initiate appropriate commands. The GPS services can also be disconnected by jamming attacks.

Protocol conversions compatible with IEC 61850

The rollout of IEC 61850 solutions have to coexist with other legacy protocols, at least during the transition phase, creating a need for harmonization between the various standards. For instance, the PMU system widely follows the IEEE C37.118.2 standard, and there is reported work on a gateway converter, with libraries that can serve as an interface between both standards based on the guidelines given in IEC 61850-90-5 [109]. Similarly, the SNTP protocol is advised for the time synchronization of devices inside substations, according to IEC 61850, but the PTP protocol, as per IEEE 1588, is also being implemented in practice due to some of its advantages over the SNTP protocol [110, 111]. PTP protocol is more accurate, in the nanosecond range, and has integrated security features such as authentication and message protection. On the other hand, SNTP protocol is less accurate, in the microsecond range, and does not encompass security aspects. These conversions will be required and used, as long as IEC 61850 does not phase out the other protocols, adding complexity to the system and potentially widening the attack surface.

Data modeling in the IEC 61850 standard

In IEC 61850, all the physical devices are logically modeled to allow interoperability among devices, independent of their type and manufacturer [91] via data objects and

their functions (data attributes), as shown in Figure 2-17. The standardized data models communicate through standardized messages via an abstract communication service interface (ACSI). This is the main feature of this standard, which raises it from the level of communication standard only. All the defined data models at the logical level in a power utility ensure not only interoperability, but also guarantee future extension of the system. This characteristic of the standard has advantages, but it can also open doors for the attackers to modify the logical data models of the power devices and system by accessing the communication network. Hence, the data model is discussed below in order to highlight the vulnerabilities from a cyberattacker's perspective. The hierarchy of the data model, as per the standard, is divided into five levels:

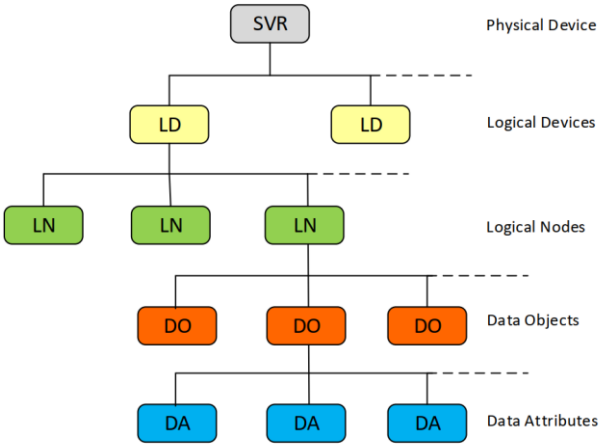


Figure 2-17. Data model in IEC 61850 [91]

1. Physical device (server or SVR): Represents the physical outlook of the domain;
2. Logical device (LD): Represents groups of functions in the domain;
3. Logical node (LN): Represents an individual group (e.g., hydropower plant, switchgear);
4. Data object (DO): Represents the devices in a group (e.g., CTs and VTs in switchgear); and

5. Data attribute: Represents the function of individual devices (e.g. current measurement by CTs).

A system event in this standard is communicated by a dataset (DS) that is basically a reference to one or more data attribute(s), as per the event to be communicated between the server and the client. The communication service is done by the appropriate messages (GOOSE/SV) based on the DSs. Hence, the DOs and attributes can be grouped in multiple ways to generate different DSs. Therefore, the optimal framing of the DSs, when DOs are updated, can reduce the transfer times between the sender and receiver. On the other hand, this characteristic can be exploited by an attacker via MITM and FDI attacks. They could generate DSs in a malicious way by referencing unwanted data attribute(s) for either false reporting of events or to increase the transfer times of the messages in order to degrade system performance. Another way would be to attack the data attributes of different DOs in the logical node hierarchy.

Vulnerabilities in substation hardware (IEDs) and software (SCL)

The periodic communications from the publisher to subscriber IEDs (specifically GOOSE messages) are prone to spoofing attacks in which the DS fields of the messages are either duplicated or tampered with, resulting in the incorrect operation of the subscribers [112]. IEDs have a generally limited processing power and flexibility that permits only hardcoded usernames and the use of simple and insecure protocols. Hence, corporate IDSs are not feasible for time-critical GOOSE messages. Hence, an attacker will usually have to intercept only the communication to/from the IEDs, as corporate IDSs cannot work with such traffic. Another way would be to change the publisher/subscriber status of the IEDs by changing the fields other than the DS (e.g., the destination/source address fields), as shown in Figure 2-18. This would disturb the hierarchy of the IEDs, forcing them to malfunction.

Destination address	Source address	Priority tagged	Ethertype	APPID	Length	Reserved 1	Reserved 2	Data	FCS

Figure 2-18. Ethernet data frame [53]

Substations might have backup IEDs for critical power devices (e.g., feeders), which become operational if the primary fails [113]; however, in the IEC 61850-standard-based substations, it is possible to create a pool of backup IEDs that can be called into service when required for any protective device whose primary has malfunctioned. The advantages are flexibility and cost-saving, although this situation can be exploited by an attacker by disengaging the backup pool of IEDs via DoS attacks. If successful, the substation equipment will not have any backup protection, and any fault that is not handled by the primary will damage the equipment directly.

The SCL file format standardizes the device configuration on one end, while it can be misused by an attacker to compromise IEDs by changing their settings. Lim [114] proposed that one IED was enough for the successive testing of multi-vendor IEDs during maintenance. Hence, if two IEDs are mapped with the same LN, they can be replaced, and the neighboring IEDs can be informed of this replacement by configuring their IED files (.CID) using system configurator (SC) and IED configurator (IC) software in the console. This approach benefits from the flexibility of LNs and SCL files, as per the IEC 61850 standard. The same flexibility can be exploited for a cyberattack by changing the logical structure of the devices connected in the substation. For instance, the status of the IEDs can be changed from ON to OFF, as shown in Figure 2-19.

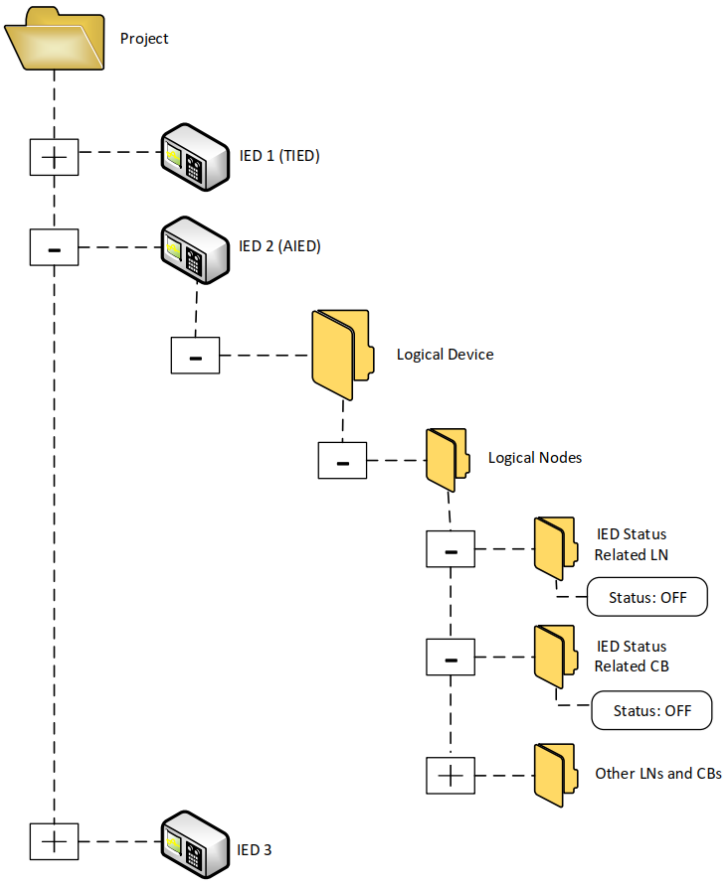


Figure 2-19. Changing status of IED in LN hierarchy [114]

The functional information of all the devices is available in the substation configuration file (.SCD). The required change in the logical structure is updated in two SCL files (.SSD and .ICD), which are fed to the SC to generate a new .SCD file for the particular substation. Inside the substation, this .SCD file is processed by the IC, and it updates the .CID files for the targeted IEDs.

Coordinated attacks

Coordinated attacks are launched in small time windows with the intention of paralyzing the complete recovery of the substation(s). The operator will still be combating the initial attack when the attacker introduces successive attacks to effect a complete loss of control by the operator [102]. Such attacks can be load redistribution (LR) attacks, combined with attacks on generators and/or lines. LR is a practical example of an FDI attack in which only load demand and line power flow values are

fabricated from state estimations in stealth mode [115]. The operator dispatches new unwanted load arrangements based on the available false data.

At this stage, it is worth summarizing the global attack methodology followed by cyber attackers to attack an electric substation. Basically, the attack vector is developed based on the two main steps an attacker will likely take to launch a cyberattack(s) on a substation. First is to access the substation network, during which attackers look for available weaknesses in the system (e.g., previous versions of operating systems) or decoy personnel (e.g., phishing emails, flash drives), using specifically-designed tools (e.g., malware). Once they gain access to the electronic parameters of the substation, they can disrupt the power being fed to the consumers by meddling with the communications from/to the substation. Another exploitation at this point could involve the architecture of the substation, including both devices and firmware. This is usually achieved by initiating coordinated attacks on the substation to keep the operator(s) away from taking any timely measures for recovery and/or isolation actions. The different attacks that we have surveyed by using the AVD taxonomy can now be classified as presented in Table 2-4:

Table 2-4. Taxonomy of cyberattacks for electrical substations.

Attack		Vulnerability (attack surface)	Damage (impact)		
Target	**Action**		**State**	**Performance**	**Severity**
Accessing substation network	Spoofing	Configuration: Poorly configured gateways and firewalls	I	Accuracy	MH
	Dictionary attack	Implementation: Weak passwords	C	Timeliness	M
	Modbus/DNP3 network scanning	Scanning of IP addresses, ports & services	IA	Timeliness	L
	Decoy shells	Specification: Old OSs	CI	Precision	M
	Malware	Specification: USB flash drives	CI	Timeliness	MH
	Worms	Implementation: Network	CIA	Timeliness	MH
	Malware, MITM	Specification: Shared internet	CI	Accuracy	H
	Phishing emails	Implementation: Weak network segmentation	CI	None	LM
	DoS	Specification	A	All	H
Exploiting features inside the substation		Communication messages			
	FDI, relay, MITM	GOOSE	CI	Accuracy	M
	FDI	SV	I	Accuracy	LM
	DoS	MMS	A	Precision	MH
	Spoofing, jamming	SNTP	IA	Accuracy	LM
		Data models			
	FDI, MITM	LNs	CI	Accuracy	MH

Attack		Vulnerability (attack surface)	Damage (impact)		
Target	**Action**		**State**	**Performance**	**Severity**
	FDI	DSs	I	Accuracy	M
		Hardware/software			
	Replay, MITM, FDI, DoS	IEDs, MUs	CIA	Precision	MH
	Malware, DoS	HMI	CIA	All	H
	Popping the HMI	SCL	CIA	Accuracy	H
		Nature of attacks			
	LR + line and/or generator attacks	Coordinated	CIA	All	H

In the state column, C stands for Confidentiality, I for Integrity and A for Availability. In the Severity column, L is for low, M for medium and H for high. The origin subcategory under attack is not added as mostly the focus is on remote attacks using the advanced communication capabilities of modern substations.

2.3.5. Countermeasures development for electrical substations

In order to come up with effective counter measures to the aforementioned attacks, it is vital to identify the critical attack paths on the substation with their effects, in a risk assessment fashion. This process is well explained by the terminology of the RAIM framework [103, 104] which identifies the following four areas to design a cyber-security solution for substation and / or the power grid:

1. **R**eal-time monitoring
2. **A**nomaly detection
3. **I**mpact analyses
4. **M**itigation

A semantic analysis framework [78, 116] has been developed for different types of cyberattacks. The purpose is to monitor the network traffic and analyze it for hostile behaviours. Impact analyses, acknowledges that attacks are bound to happen, but when they do happen, the parts of a substation having major impact should remain secure and the cyberattacks should be directed (lured) towards less critical paths until full restoration of the substation. Based on such analyses, the mitigation or countermeasures to the cyberattacks are designed for electrical substations. Such analyses in substations are done via power flow studies in which causes and effects of different interruptions are analyzed. The detection accuracy and latency of such analysis are of paramount importance to avoid cascading failure or collapse of the power grid originating from electrical substations [116].

The countermeasures against cyberattacks intended for the state estimation in specific are divided into two broad categories i.e. protection-based and detection-based [117]. The former method is to protect the critical sensors with hardware upgrades which add cost to the system. The latter method is to observe the measurements to detect and rule

out bad data. This detection of bad data can be done either by energy functions (dissipativity-based) or by the residuals of predicted and observed values (observer-based). Arturo et al. proposed an innovation approach to detect malicious data attack without requiring the past knowledge of the attack [42]. Another category of countermeasures in smart grids is based on game theory where adversary (attacker) and defender (operator) game models are used for decision making based on Nash equilibrium. M. Touhiduzzaman et al. employed diverse security mechanism inside the electronic parameter of substations using graph-based coloring game [118]. The security mechanisms are custom made and are based on firewalls and VPNs.

Countermeasures to substation's network attacks

The intelligence gathering or real time monitoring of the processes in a substation is the key to interrupt the expected cyberattacks in future. Successful interruption in the path of attacker's learning can avert his harmful actions on the system [119]. Moreover, by identifying and protecting the few critical paths, buses and components in a substation, the affected level can be reduced to a minimum in case of an unavoidable cyberattack. This element should be the mandatory for the recovery algorithms which become active on incident reporting of successful intrusions into the electrical substations. The same concept can be extended to pivotal substations that can initiate cascading failure and ultimately blackout. Cyber intrusions on such substations can be thwarted by unidirectional gateways which would isolate the plant from outside attacks [52].

Distributed energy resources and microgrids based on mostly renewable energy sources, working on or off the grid also improve resiliency of the smart grid in case of cyberattacks as compared to centralized distribution systems [58, 120]. The modern substations are based on IEC-61850 allowing remote communication of heterogeneous devices for monitoring and control. Hence, software defined networking (SDN) is

proposed to secure the communication [92]. The purpose of the networking is to isolate traffic, detect anomalies and place firewalls and spoofing controls.

At this stage, the attacker is outside the electronic parameter of the substation wanting to access its network by either wireless hub or modem penetrating the firewall. This is achieved by the weaknesses present in the substation as discussed earlier. The countermeasures at this step can be to employ IDS/IPS monitoring malicious network attempts and intrusions which can be averted using VPNs, honeypots and by custom made solutions designed for specific known attacks. The network attacks with associated countermeasures are summarized in Figure 2-20.

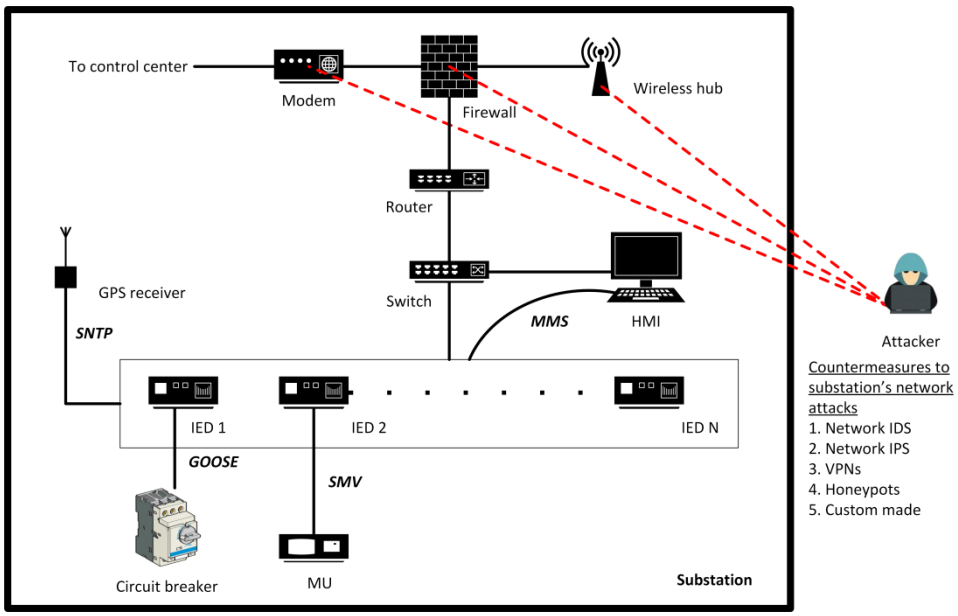


Figure 2-20. Countermeasures to substation's network attacks

Countermeasures to substation's data attacks

The state variables and power system parameters can be forecasted with acceptable accuracy using modern hybrid algorithms such as HHT-SVM and HHT-ANN models based on hybrid Hilbert transform, support vector machine and neural networks [121]. The predicted values are based on historic data of operations of the system and can become a decider factor in case of cyberattacks. As the cyberattacks tend to modify the

state variables or system parameters in case of injection attacks, hence, the prediction matrix can generate alerts of such deviations which can be stopped by operators or IPSs. Depending on the risk analysis of the vulnerabilities being discovered by the attacker, the magnitude and time of cyberattacks can also be forecasted based on nature inspired algorithms.

The time critical messages in IEC-61850 based substations such as GOOSE and SV are made more secure by implementing their routable versions known as R-GOOSE and R-SV [38, 109]. N. H. Ali et al. improved the performance of communication network by fast tripping in electrical substations using travelling wave phenomenon [122]. Lazaro et al. proposed software for anomaly detection in GOOSE messages intended for IEDs in real time inside a substation [112]. The new method is capable of capturing counterfeit GOOSE messages which were escaped by the standard IDSs. The security of GOOSE messages inside electrical substations are also increased by employing Secure Hash Algorithm (SHA-1) [47].

At this stage, the attacker has breached into the substation's network narrowing down his focus on the communication between the devices inside the substation. The time critical messages such as GOOSE (performing protection operations) are the primary target in addition to the communication originating from HMI, IEDs and GPS receiver. In order to secure the data communication between the substation devices, methods such as encryption, cryptography, key management and custom made can be deployed. The communication protocols themselves can be added with security by using their routable versions such as R-GOOSE and R-SMV. The data attacks with associated countermeasures are summarized in Figure 2-21.

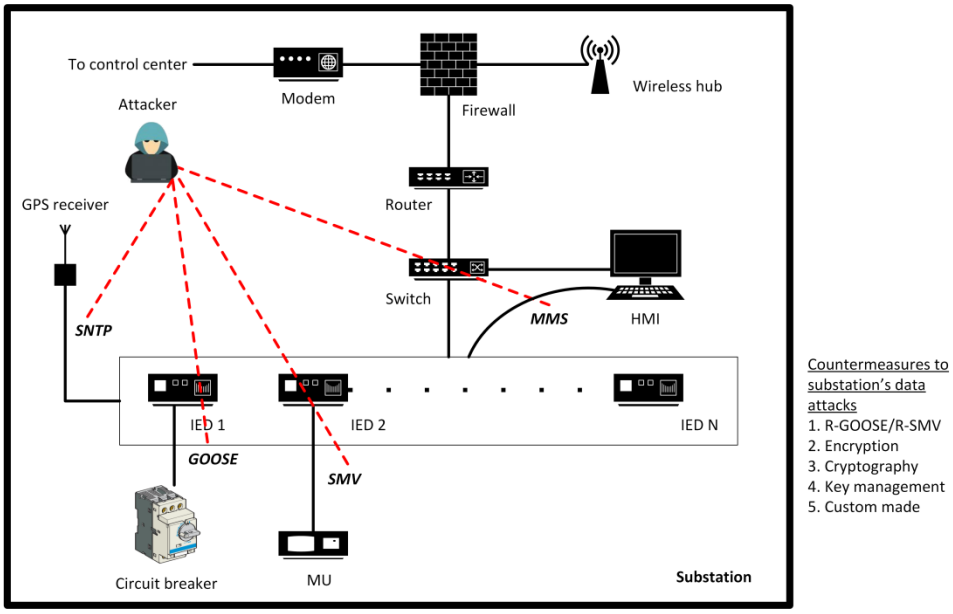


Figure 2-21. Countermeasures to substation's data attacks

Countermeasures to substation's devices attacks

The devices in a substation are not secured properly and are a target of implementation attacks. The communication security at embedded device level as shown in Figure 2-22 is also not focused in IEC 62351. The issue has been discussed in [123] and its corresponding impact on the power grid. For the implementation attacks, the security at embedded device level is required. As the most targeted device of attackers in a substation is IED, hence its security is proposed in recent literature using different algorithms and embedded IDS in the IEDs for different attacks related to GOOSE and SV messages [123]. The focus is to accurately and timely detect the abnormal behaviors in the received messages without any impact on the protection functions of the IEDs. Moreover, the fabricated confirmation of the messages can be detected by authentication code between the IEDs [54]. The anomalies in the messages of substation communication can be detected by IEDs by comparing the structure with previous normal messages and by evaluating the impact of the control actions on the system. If the messages have significant deviation with larger impact, then the corresponding

IEDs can block such control commands [54]. This blocking feature can either be programmed using some algorithm or can be delegated to operators to take appropriate actions.

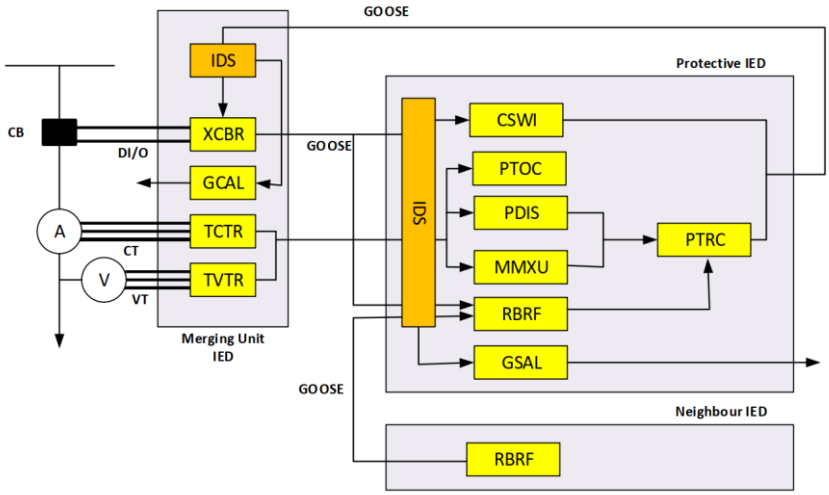


Figure 2-22. IED protection with embedded IDS [54].

A corporate developed IDS or IPS would be ineffective for IEDs protection in modern substations. Hence, custom made solutions targeted for specific purposes are being developed and proposed by researchers in the academic circles. Seongil Lim exploited the substation configuration language to provide protection measures inside electrical substations [114]. The attacks to the power grid cannot be avoided; hence a twofold approach is suitable to counter the disturbances and damages caused to power system. Firstly, the efforts and solutions are devised to protect the system from such attacks. Secondly, upon incident of such attacks, the optimal power flow is conducted by considering the consequences of attacks using computational intelligence methods [59]. This step minimizes the harmful effects of the attacks as optimal strategies are adopted based on the power flow. The robustness of the system is also increased by such analyses in case of cyberattacks [52, 70].

The second target (other than data communication between devices) after accessing substation's network is the devices themselves, installed within the substation.

Different IEDs are operating in the substation performing measurements, protection and control commands both in normal and fault conditions. The devices can be made to malfunction by corrupting their firmware or data storage. The IEDs can be programmed with embedded security as discussed. Also role based access control (RBAC) can be deployed to make sure the access to these important IEDs is limited to authorized personnel only. Various custom made methods dedicated to specific IEDs based on their history of operation and lesson learned can be another solution. The devices attacks with associated countermeasures are summarized in Figure 2-23.

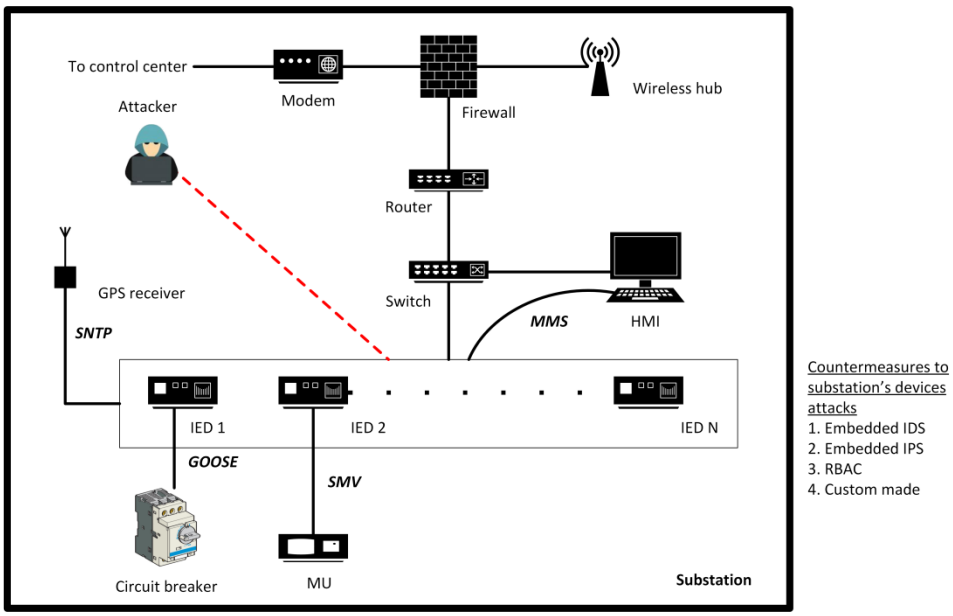


Figure 2-23. Countermeasures to substation's devices attacks

Custom made countermeasures for electrical substations

In addition to the previous generic countermeasures, many researchers propose different novel techniques to avoid or limit specific cyberattacks on electrical substations and power grid. Jiaqing et al. proposed a network scheme for the process bus in electrical substations eliminating the need of external clock for GPS signals [111]. As the scheme is local, it will be difficult for the attackers to forge timestamps through spoofing attacks. Zhou et al. proposed an ensemble based algorithm for

anomaly detection in the synchrophasor data of PMUs [124]. The algorithm can train itself based on past data and can distinguish events from bad data. Hence, the cyberattacks by injecting false data over the PMUs based IEDs can be prevented. Yingmeng et al. also proposed optimal strategies based on game theory for coordinated attacks on electrical substations [115]. The attack examples are load redistribution in coordination with attacking generators / lines by modifying the data in state estimation matrix. Seongil Lim proposed a testing method for the IEDs in live substations based on IEC-61850 standard [114]. The method can be utilized to analyze IEDs in case of cyber attacks to take proper actions. Hyung Lim et al. proposed a local backup IED scheme in case of simultaneous faults on protection IEDs in modern substations [113]. Bassam et al. proposed detection and mitigation technique for the delay attacks targeted on precision time protocol (PTP) which is responsible for accurate time stamping of measurements and events [110]. Suahil et al. proposed a novel communication architecture based on parallel redundancy protocol (PRP) with zero switchover time for IEC 61850 based substations [85]. The protocol is inspired and directed by IEC 62439-3 standard to be used in substation communication networks for rapid system recovery during faults. The same concept can be extended as a new countermeasure to be implemented against cyber attacks. Junsik et al. proposed an intruder detection method by analyzing malicious packets in IEC 61850 based substations [125]. FPGA board with Xilinx was used to design a complex rule matching module using Shift-And algorithm. The discussed countermeasures are summarized in Table 2-5 corresponding to their attack types and characteristics.

Table 2-5. Characteristics of custom made countermeasures in reported literature

Description of countermeasure	**For network attack**	**For data attack**	**For device attack**	**Characteristics**
Network scheme for process bus for GPS signals [111]	✓	✓	×	To prevent spoofing attacks
Algorithm for anomaly detection in PMUs' data [124]	×	✓	×	To prevent false data injection attacks
Game theory based optimal strategy for coordinated attacks [115]	×	✓	×	To prevent load redistribution attacks
Testing methods for IEDs [114]	×	×	✓	To analyze IEDs in case of attacks in real time
Local backup scheme for IEDs [113]	×	×	✓	To prevent simultaneous faults on protection IEDs
Detection and mitigation technique for PTP [110]	×	✓	×	To prevent delay attacks
Novel communication architecture [85]	×	✓	×	Rapid system recovery during faults
IDS to analyze malicious packets [125]	×	✓	×	To secure data communication between devices

Basically, from attacker perspective to attack a substation, his first objective will be to hook into the substation's network remotely by exploiting the weaknesses (vulnerabilities) himself and/or by the help of insiders by launching miscellaneous attacks to damage and effect the system and processes. Once, he gets the access to substation network, the next exploitation(s) and attack will be on the data communication and devices within the substation. This stage can also increase the severity of the attack based on the knowledge and objective of the attackers. The logical countermeasures to the attacks in these stages are summarized in Table 2-6.

Table 2-6. Countermeasures with attack type in electrical substations corresponding to taxonomy of attacks with AVD model.

Attack				
Target	**Action**	**Vulnerability (attack surface)**	**Attack type**	**Countermeasures**
Accessing substation network	Spoofing	Configuration: Poorly configured gateways and firewalls	Network	Network IDS, IPS
	Dictionary attack	Implementation: Weak passwords	Network	Cryptography
	Modbus/DNP3 network scanning	Scanning of IP addresses, ports & services	Network	VPNs, Honeypots
	Decoy shells	Specification: Old OSs	Network	Antivirus, IDS, IPS, Custom made
	Malware	Specification: USB flash drives		
	Worms	Implementation: Network		
	Malware, MITM	Specification: Shared internet		
	Phishing emails	Implementation: Weak network segmentation		
	DoS	Specification		
Exploiting features inside the substation		Communication messages		
	FDI, relay, MITM	GOOSE	Data	R-GOOSE, R-SMV, Key Management
	FDI	SV	Data	
	DoS	MMS	Data	Cryptography, Encryption, RBAC

Target	Attack Action	Vulnerability (attack surface)	Attack type	Countermeasures
	Spoofing, jamming	SNTP	Data	Custom made
		Data models		
	FDI, MITM	LNs	Data	VPNs, Honeypots
	FDI	DSs	Data	
		Hardware/software		
	Replay, MITM, FDI, DoS	IEDs, MUs	Device	Embedded IDS, IPS
	Malware, DoS	HMI	Device	RBAC
	Popping the HMI	SCL	Data	Custom made
		Nature of attacks		
	LR + line and/or generator attacks	Coordinated	Device	Custom made

The column Damage is included in Table 2-4 and is hence not provided here.

2.3.6. Cybersecurity solution for electrical substations

The lifecycle of cybersecurity consists of prediction, protection, detection and reaction cycles [126]. Prediction and detection is done by collecting intelligence / risk assessment and intruder detection of the considered system. The remaining two active cycles i.e. protection and reaction are achieved by software and hardware based on mitigation and recovery techniques to neutralize such threats. In power system and electrical substations, SCADA and SAS are the most favorite targets of the attackers. The countermeasures to cyberattacks can be classified as legal, technical, organizational, capacity building and cooperation [126]. The classifications other than technical correspond to respective institutions and involve legislation, policy making, certifications and audits. The technical countermeasures, is a topic for the academic researchers to contribute different methods and ideas that can counteract the prevalent cyberattacks to the energy sector.

The complex and heterogeneous power system of today intertwines electrical equipment with IT equipment known as cyber physical power systems (CPPSs) as shown in parallel in Figure 2-24. The cyber layer is controlling the physical layer through IEDs which control protection and measurement devices (circuit breakers and merging units respectively). The black boxes on the left diagram correspond to the circuit breakers which are shown on the bottom of the right figure. This system is often modeled to understand the interaction and its response as a whole to different modeled faults and cyberattacks which results in better understanding of the complex system and its reaction to different abnormal and hostile behaviors. As a result, different countermeasures and mitigation techniques can be proposed. The objective of such models is to simply represent the interaction between power and cyber systems and both the internal and external faults on the system. For this purpose, models based on

graphs, mechanics, probability and simulation have been developed in the reported literature [59]. Maggie et al. conducted the vulnerability analysis using graph theory by considering power flows and topological analysis of a power grid [127]. After careful evaluation of the system, the countermeasures are also proposed based on network theory, control theory, probability, analytical, optimization and simulation methods.

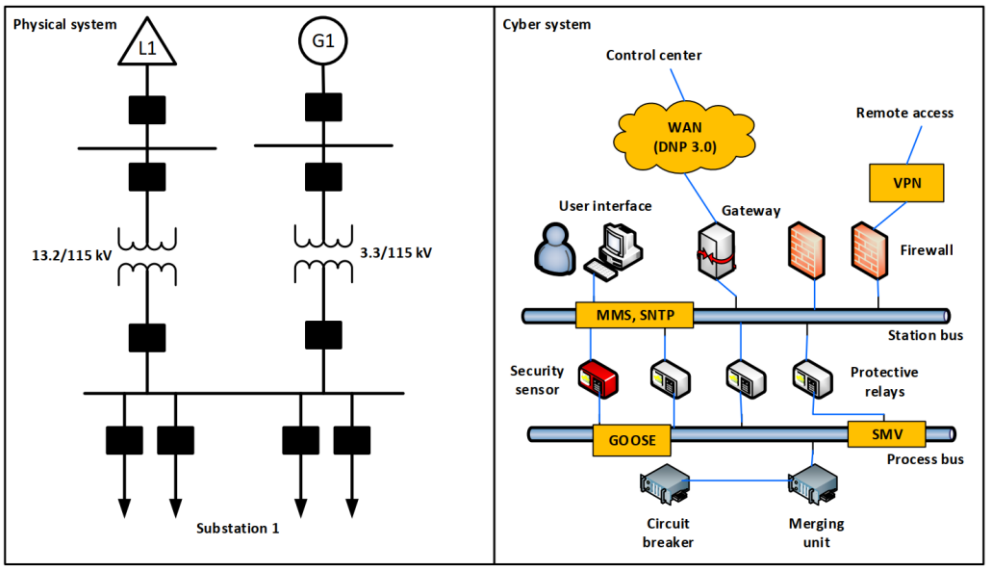


Figure 2-24. Physical and cyber layers in a substation [97].

The technical countermeasures are based on network, data and device security in the electrical substations of the power grid. The software measures include intruder detection / prevention systems (IDSs /IPSs) on the substation network and also embedded on the devices such as IEDs in a substation. The latter adds significant cost to the system but it is worth doing and various methods can be proposed for cost reduction which is acceptable to threats level of the cyberattacks. Other than this, firewalls, antiviruses and antimalware are also employed for protection purposes. Regarding the data security, concatenation of security tags or message authentication code (MAC) to substation specific messages such as GOOSE, MMS and SV is another effective technique to distinguish malicious packets from the normal traffic [53]. Hence, to develop a cybersecurity solution; cyber threat intelligence, traceback,

honeypots, live forensics, network forensics and malware analysis are important attributes of cyberattacks to consider for developing the solution [126].

The cyberattacks on modern substations are often carried out using different malware. Peter et al. conducted extensive review on malwares reported to effect critical infrastructures [128]. They concluded their research by analyzing different attributes of practical malwares to give appropriate countermeasures. These measures can be extended and employed to a smart grid for cybersecurity protection of electrical substations in a smart grid. They include Security Updates, Heuristic Detection, Avoid Monocultures, Resilience Measures, Fallback Systems, Emergency Restore, Anomaly Detection, Strict Firewall Rules, Access Management, Content Filtering, Social Engineering Education, Network Segmentation & Event Correlation and Network Segmentation to Type of Service. Security filters based on symmetric cryptography, are another countermeasure to secure substation communication by employing them between IEDs and communication buses in IEC-61850 based substations [129]. The filters can be designed to fulfill the stringent time requirements of critical messages in modern substations.

Overall, a robust cybersecurity solution is suggested for electrical substation that should be composed of probes (Snort and Bro software), network sensors, intruder detection / prevention systems, honeypots including honeynets and darknets, mediation devices, security information and event management (SIEM) and graphical user interface (GUI). The overall system is shown in Figure 2-25 [130] which was designed for the generation side of power grid and is applicable and can be implemented for distribution electrical substations. The cybersecurity protection system (CPS) operates through control and supervisory substation (CSS) as its center. The normal operations are monitored and controlled by SCADA system while IDS is reserved for unauthorized and remote

network intrusions. Hence, SCADA will be dedicated for system faults located in the incoming or outgoing network or even inside the substation itself while IDS monitors the network traffic from WAN, enterprise network and external systems such as vendors. CPS consists of following five components:

1. ***Analysis Modules*** analyzing system faults and malicious network accesses sensed by SCADA and IDS probes respectively,
2. ***Honeypots*** emulating physical equipment of power grid to divert unexperienced/disgruntled employees and attackers from harming real equipment by SCADA and IP honeypots/darknets respectively,
3. ***Maintenance Server*** for conducting active and preventive maintenance securely,
4. ***GUI*** consisting of a server to display the live diagram of the substation and
5. ***SIEM*** consisting of a server and database storage for monitoring and control of substation events.

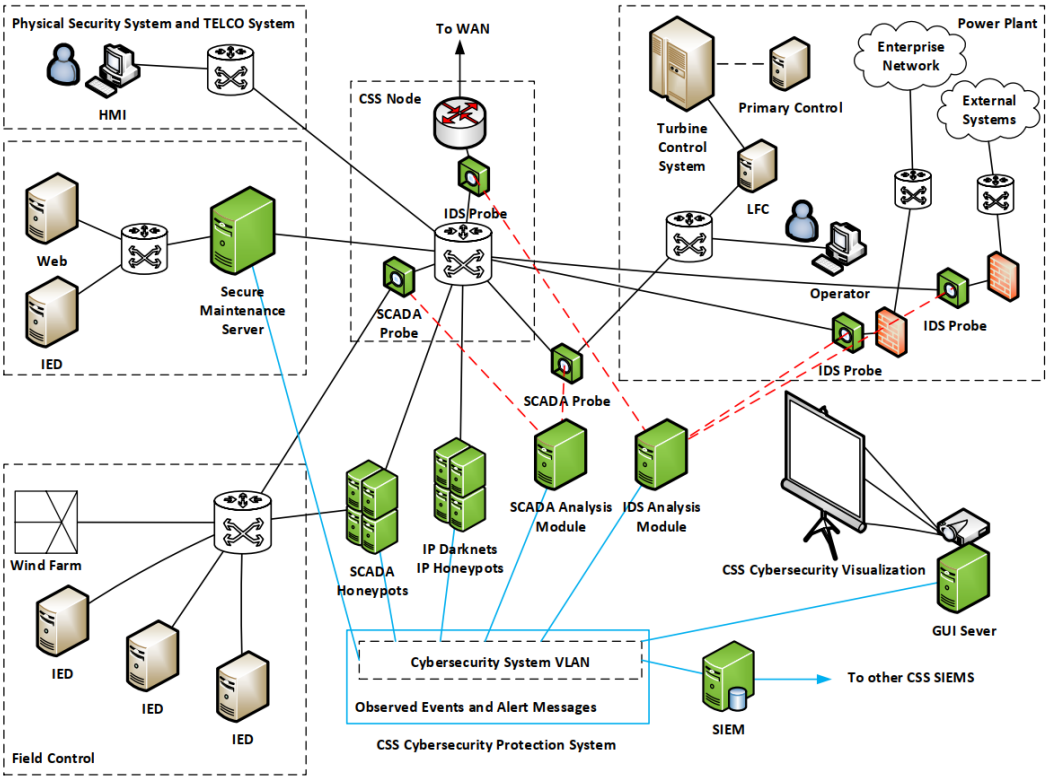


Figure 2-25. Cybersecurity protection system [130].

The probes, network sensors and honeypots try to eradicate the cyberattacks initiated towards the power grid by diverting them towards emulated devices. However, if an attack manages to affect the real equipment in a power grid then during the attacks, ethical hacking can be utilized to counter the effect of the attackers by the defenders. Forensic Science is implemented after the attack is neutralized to find the root causes, document the lessons learned and for critical updates of the system to prevent from such attacks in future. Having said that, the distribution electrical substations are continuously evolving, and IEC-61850 is accordingly being revised and extending its scope in the power system. This evolution requires to practically investigate the network, data and devices of modern substations and accordingly design a cybersecurity testbed based on the guidelines discussed in this section.

2.3.7. Summary

In this work, smart grid security with a focus on electrical substations is investigated

from the perspective of a cyberattacker. Examples of cyberattacks in the energy sector are given and the differences between traditional and modern substations are clarified. In particular, the standards that are (or will soon be) implemented and how they encompass security are discussed. The general steps of a cyberattack are summarized, and classified them in terms of a main attack vector. Moreover, the current developments in electrical substations were analyzed in order to describe the weaknesses in the substations that can become attack surfaces. The literature to map known attacks is reviewed extensively, in terms of the steps an attacker will likely follow in order to remotely breach an electrical substation. The attack vectors are tabulated, based on an attacker's perspective, in order to penetrate the electronic boundary of a substation by accessing the network first and then exploiting the system more deeply after the intrusion. The defined attack vector resulting from this study could be a basic tool for future studies to use to systematically assess the security of substations against such known attacks. The countermeasures to such attacks are then discussed in the light of the new IEC 61850 standard, which is being adopted worldwide for substation automation. The countermeasures have been categorized and analyzed according to their development phases culminating in a cybersecurity solution applicable to electrical substations in the end. As of future work, mitigation techniques are under work that will highlight the impact of such attacks in the case of protocols that have already been deployed, such as DNP3, IEC-60870-5-104 and IEC-61850. A holistic cybersecurity solution addressing the concerns of communication and power domains is still a challenge requiring experimental study and will be tackled in our future work.

CHAPTER 3: IMPLEMENTATION AND COMPARISON OF PARTICLE SWARM OPTIMIZATION AND GENETIC ALGORITHM TECHNIQUES IN COMBINED ECONOMIC EMISSION DISPATCH OF AN INDEPENDENT POWER PLANT

3.1. Introduction:

This chapter presents the optimization of fuel cost, emission of NO_X, CO_X, and SO_X gases caused by the generators in a thermal power plant using penalty factor approach. Practical constraints such as generator limits and power balance were considered. Two contemporary metaheuristic techniques, particle swarm optimization (PSO) and genetic algorithm (GA), were simultaneously implemented for combined economic emission dispatch (CEED) of an independent power plant (IPP) situated in Pakistan for different load demands. The results are of great significance as the real data of an IPP is used and imply that the performance of PSO is better than that of GA in case of CEED for finding the optimal solution concerning fuel cost, emission, convergence characteristics, and computational time. The novelty of this work is the parallel implementation of PSO and GA techniques in MATLAB environment employed for the same systems. They were then compared in terms of convergence characteristics using 3D plots corresponding to fuel cost and gas emissions. These results are further validated by comparing the performance of both algorithms for CEED on IEEE 30 bus test bed.

3.2. Problem Formulation:

CEED comprises two objective functions (cost and emission) that are to be minimized. The fuel cost and emission of a generator can be represented as a quadratic

function of the generator's real power [131]. Hence, for *N* running generators in a plant, the total fuel cost (*FC*) and emission of a single gas (E_g), respectively, are given in Equations (1) and (2).

$$FC = \sum_{i=1}^{N} F_i(P_i) = \sum_{i=1}^{N} (a_i P_i^2 + b_i P_i + c_i) \tag{3-1}$$

$$E_g = \sum_{i=1}^{N} E_i(P_i) = \sum_{i=1}^{N} (\alpha_i P_i^2 + \beta_i P_i + \gamma_i) \tag{3-2}$$

where a_i, b_i, and c_i are cost coefficients; α_i, β_i, and γ_i are emission coefficients of unit *i* out of *N* generators. They are computed by the following:

- Getting the heat rate curves and emission reports of operational generators from the plant.
- Then, calculating and arranging their fuel costs and emissions corresponding to their active powers in tabular form.
- Applying the quadratic curve fitting technique on these data points to get cost and emission coefficients.

This multiobjective optimization problem is converted to a single objective function of total cost (*TC*) by imposing a penalty *(h_g)* on the emission of *G* gases to convert them into emission cost (*EC*).

$$TC = FC + EC = FC + \sum_{g=1}^{G} h_g \times E_g \tag{3-3}$$

There are different types of penalty factors; their benefits and drawbacks are thoroughly discussed in [132]. The min–max penalty factor of Equation (4) is used in this work because of its superiority reported in [132] over the others.

$$h_i = \frac{F_i(P_{i,min})}{E_i(P_{i,max})} = \frac{a_i P_{i,min}^2 + b_i P_{i,min} + c_i}{\alpha_i P_{i,max}^2 + \beta_i P_{i,max} + \gamma_i} \tag{3-4}$$

where h_i for each generator for every gas is calculated and all are sorted in ascending order, then starting from the smallest h_i, $P_{i,max}$ of corresponding generator is added until $\sum P_{i,max} \geq P_D$, the h_i at this stage is selected as penalty factor h_g of that gas for the given load demand.

For achieving this optimization, the *N* generators will be dispatched with various combinations of output powers but each combination must conform to two mandatory constraints. First of all, no unit should violate its limits for producing output power *(P_i)*, and secondly the total generation *(P_G)* should meet the load demand *(P_D)* and transmission line losses *(P_L)* [131].

$$P_{i,min} \leq P_i \leq P_{i,max} \tag{3-5}$$

$$P_G = \sum_{i=1}^{N} P_i = P_D + P_L \tag{3-6}$$

The generator limits constraint is satisfied by initializing each unit's power within prescribed limits and then constantly checking the violation. If a unit crosses its limit, then its output is set to that limit. The second power balance constraint is accounted for by letting algorithm to find optimal powers for *N–1* generators and setting the power (P_N) of last generator *N* also called slack generator to:

$$P_N = (P_D + P_L) - \sum_{i=1}^{N-1} P_i \tag{3-7}$$

If losses are ignored, then the power of slack generator will reduce to:

$$P_N = P_D - \sum_{i=1}^{N-1} P_i \tag{3-8}$$

3.3. Implementation of PSO to CEED:

J. Kennedy and R. Eberhart proposed this method in 1995 after observing and modeling the social interaction within bird flocks and fish schools for searching food [133]. The particles in such swarms move to attain optimal objective (food) based on their personal (*pbest*) and swarm's (*gbest*) best experiences. Each particle is a valid solution to the problem, and hence, its dimension is that of problem space. The position of each particle keeps on updating by its current velocity, particle's best position, and swarm's best position until the optimal solution is discovered. The velocity and position of the particle is given by Equations (9) and (10).

$$v_j^{k+1} = \mu^k v_j^k + c_1 r_1 \left(pbest_j - x_j^k\right) + c_2 r_2 (gbest - x_j^k) \tag{3-9}$$

$$x_j^{k+1} = x_j^k + v_j^{k+1} \tag{3-10}$$

where j is particle counter, k is iteration counter, c_1 and c_2 are acceleration coefficients, r_1 and r_2 are random numbers in the range of 0–1, $pbest_j$ is the best position of particle based on its personal knowledge, *gbest* is the best position of particle based on group knowledge, and μ is the inertia weight given by Equation (11).

$$\mu^k = \mu_{max} - \left(\frac{\mu_{max} - \mu_{min}}{iter_{max}}\right) k \tag{3-11}$$

The performance of classical PSO has been made a lot better by working on its various parameters and by using different search strategies for updating the particle's position [131]. Hence, different variants of PSO has been introduced, such as WIPSO and TVAC-PSO, in which inertia weight μ is improved and acceleration coefficients c_1 and c_2 are timely varied [134], MRPSO [135] in which particle's position is changed by

using moderate random and chaotic search techniques, respectively. It has been observed that the most straightforward and efficient way of making classical PSO more effective is to use the constriction factor approach (CFA) [136], in which particle's velocity (9) is multiplied by a parameter called constriction factor (*CF*) given by Equation (12).

$$CF = \frac{2}{|2 - \varphi - \sqrt{\varphi^2 - 4\varphi}|} \tag{3-12}$$

where $\varphi = c_1 + c_2$ and $\varphi > 4$. The PSO algorithm for CEED, with corresponding flowchart in Figure 3-1, is implemented in the following steps:

1. Input values of fuel coefficients, generators limits, emission coefficients, load demand, maximum iterations, number of particles, acceleration coefficients, and inertia weight's maxima-minima.
2. Randomly initialize power outputs (position) of $N-1$ generators within their limits and change in these powers (velocity) for all particles.
3. Calculate the power of slack generator from Equation (3-8) to meet the power balance condition of Equation (3-6). P_N should also be within its unit's limits. If any unit out of N surpasses its boundary at any stage throughout the algorithm, it is set to the limit which it has broken.
4. Initialize *pbest* and *gbest* to infinity and find penalty factors of all considered gases.
5. Find fuel cost *FC*, emission of gases E_g, emission cost *EC* with total cost *TC* for all particles from Equations (3-1), (3-2), and (3-3), respectively.
6. Update *pbest* of each particle with its total cost if former is greater than latter. The minimum *pbest* out of all particles is stored as *gbest* if its present value is smaller than its previous value. The generators' powers corresponding to *pbest* and *gbest* are stored in separate matrices and are also modified on every update.

7. Calculate inertia weight from Equation (3-11), find new velocities and positions of *N-1* generators for all particles form Equations (3-9) and (3-10), and keep them within units' limits in case of violation.
8. For slack generator *N*, calculate its power from Equation (3-8) and this should also be in limits. If violation is done, set this power to the limit crossed and start changing the output from first generator until Equations (3-5) and (3-6) are satisfied.
9. If algorithm is converged, continue to next step, go to step 5 otherwise.
10. Print neatly the results of optimal solution *(gbest)* including powers of all generators, line losses, fuel cost, emission of gases, penalty factors, emission cost, and total cost for the given load demand.

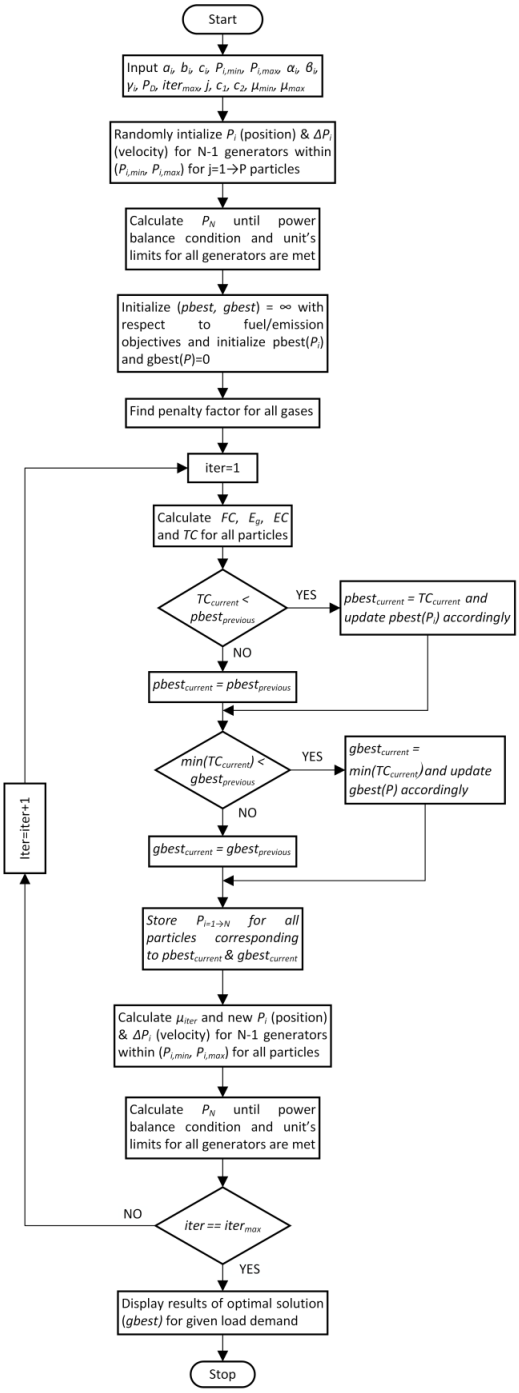


Figure 3-1. Implementation of combined economic emission dispatch (CEED) using particle swarm optimization (PSO) algorithm.

3.4. Implementation of GA to CEED:

D.E. Goldberg gave the basic theory for design and analysis of genetic algorithms based on the concept of biological evolution in 1988–1989 [137], and later, J.H.

Holland established it systematically as a fact. In genetic algorithms, the problem variables (output powers) are coded into binary strings. Each string is a valid solution to the problem and hence its length should be comparable to the problem space (number of generators *N*). The bits reserved logically for single generator's power *(genbits)* in a string is given in Equation (3-13).

$$2^{genbits} \geq Max[P_{1,max}, P_{N,max}] \tag{3-13}$$

The length of the binary string *(strlen)* will be $N \times genbits$. Each individual (string) has a fitness value in the range 0–1 which basically relates that individual to the one having maximum fitness in that population. The fitness function should be linked to the objective under discussion contrary to the constraints of the objective function which should be dealt by external checks. Considering this fact and the remarkable communication within the group by PSO parameters *pbest* and *gbest*, a new fitness function different from the one reported in [3] and [5] for j^{th} individual out of *P* individuals is given by (14).

$$fit_j = 1 - \left(\frac{pbest_j - gbest}{Max[pbest_1, pbest_P] - gbest} \right) \tag{3-14}$$

The initial population is randomly generated, keeping in view the generators' limits but the next generations are produced by selection, crossover, and mutation performed on the present one (powers corresponding to *pbest*). Selection is basically making a mating pool of fitter strings from present population based on the natural principle of "survival of the fittest." It is usually done by the concept of roulette-wheel. No new string is formed in selection phase. The greater the fitness of a string, the greater portion of the wheel's circumference it will occupy and the greater chance it will get to copy into mating pool. The wheel is spun *P* times to select a population of good parents for producing off springs by crossover and mutation.

Crossover is performed on two parents of selected population to produce two off springs. There are three types of crossover: one point, multi-point, and uniform, explained in Table 2.

Table 3-1. The types of crossover.

Item	One point	Multipoint	Uniform
Parent 1	000 00000	00 00 00 00	00 00 00 00
Parent 2	111 11111	11 11 11 11	11 11 11 11
Site/Mask	3	2, 4, 6	01 01 10 10
Child 1	000 11111	00 11 00 11	01 01 10 10
Child 2	111 00000	11 00 11 00	10 10 01 01

Crossover site is selected randomly and the probability of crossover (p_c) is usually taken higher. In this work, one point crossover is performed on selected strings of mating pool. Finally, mutation is performed on the children produced after crossover which is just flipping of the child's bit at mutation site selected randomly. Its probability (p_m) is usually taken lower, e.g., if child is (11 11 11 11) and mutation site is 4, then the mutated child will be (11 10 11 11). This journey of producing next generations continues until the optimum solution is found. The GA algorithm for CEED, with corresponding flowchart in Figure 3-2, is implemented in the following steps:

1. Input values of fuel coefficients, generators limits, emission coefficients, load demand, maximum iterations, number of individuals, *genbits* from Equation (3-13), *strlen*, p_c, and p_m.
2. Randomly initialize power outputs of $N-1$ generators within their limits for all individuals.
3. Calculate the power of slack generator from Equation (3-8) to meet power balance condition of Equation (3-6). P_N should also be within its unit's limits. If any unit

out of *N* surpasses its boundary at any stage throughout the algorithm, it is set to the limit which it has broken.

4. Initialize *pbest* and *gbest* to infinity and find penalty factors of all considered gases.
5. Find fuel cost *FC*, emission of gases E_g, emission cost *EC* with total cost *TC* for all particles from Equations (3-1), (3-2), and (3-3), respectively.
6. Update *pbest* of each individual with its total cost if former is greater than latter. The minimum *pbest* out of all particles is stored as *gbest* if its present value is smaller than its previous value. The generators' powers corresponding to *pbest* and *gbest* are stored in separate matrices and are also modified on every update.
7. Calculate fitness function for all individuals from Equation (3-14). Code the output powers to binary strings, perform the three genetic operators (selection, crossover, and mutation), and again decode them to output powers.
8. Keep all outputs within units' limits in case of violation. For slack generator *N*, calculate its power from Equation (3-8), and this should also be in limits. If violation is done, set this power to the limit crossed and start changing the output from first generator until Equations (3-5) and (3-6) are satisfied.
9. If algorithm is converged, continue to next step, go to step 5 otherwise.
10. Print neatly the results of optimal solution *(gbest)* including powers of all generators, line losses, fuel cost, emission of gases, penalty factors, emission cost, and total cost for the given load demand.

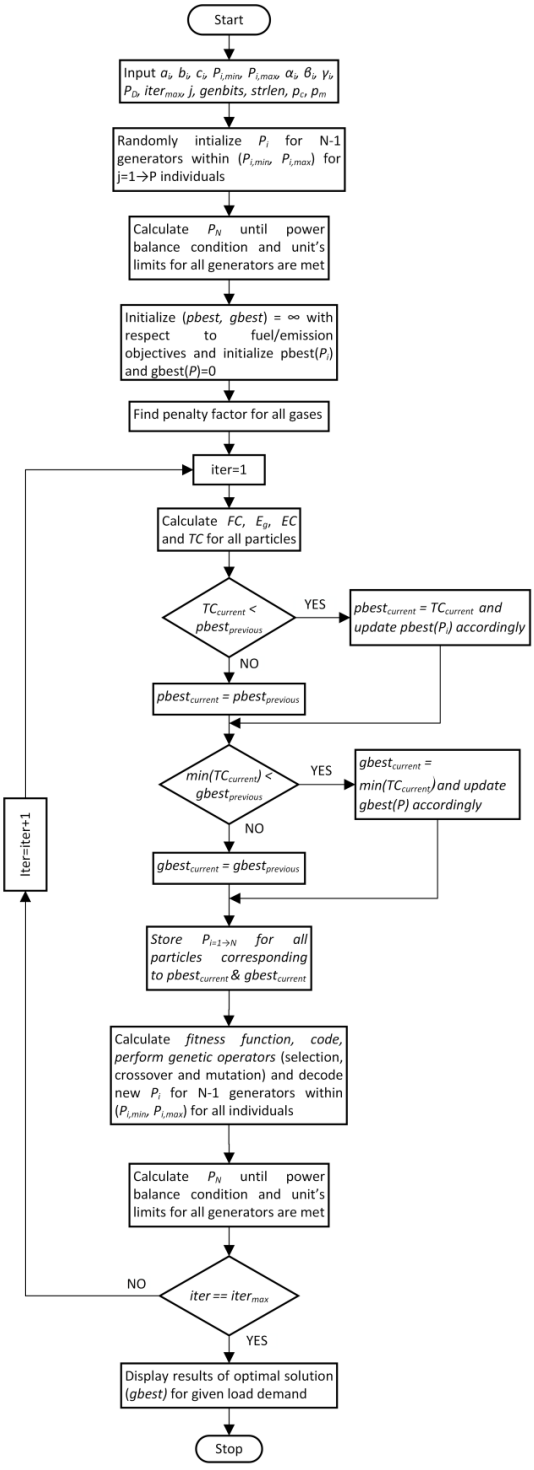


Figure 3-2. Implementation of CEED using genetic algorithm (GA) algorithm.

3.5. Simulation Results:

Combined economic emission dispatch using PSO and GA for 500 iterations were implemented on MATLAB on six generators of IEEE 30 bus system and eight

committed units (gas turbines) of an IPP in Pakistan for load demands of 1500 and 2000 MW, and 500 and 700 MW, respectively. The initial parameters set in both algorithms were:

PSO: Particles = 10, $\mu_{max} = 0.9$, $\mu_{min} = 0.4$, $c_1 = 2.05$, $c_2 = 2.05$, $\varphi = 4.1$, and $CF = 0.7298$

GA: Individuals = 10, $p_c = 0.96$, and $p_m = 0.033$

The solutions with average operating time *(t)* were selected out of 50 trials for comparison between PSO and GA.

3.5.1. IEEE 30 Bus System:

The data for fuel cost and emission coefficients were taken from [5]. Transmission line losses were not accounted for while all three gases (NO_X, CO_X, and SO_X) were considered; their penalty factors were calculated using Equation (3-4) and the procedure following this equation, for load demands of 1500 and 2000 MW given as:

$P_D = 1500$ *MW:* $h_{NOX} = 3.1669$, $h_{COX} = 0.1221$, and $h_{SOX} = 0.9182$

$P_D = 2000$ *MW:* $h_{NOX} = 5.7107$, $h_{COX} = 0.1307$, and $h_{SOX} = 0.9850$

The results are summarized in Table 3-2 (all powers are in MW, emissions in kg/h, costs in $/h, and time in seconds) while the convergence characteristics of both algorithms, with respect to both objectives (fuel cost and emission) for P_D = 1500 MW and P_D = 2000 MW, are shown in Figure 3-3 and Figure 3-4, respectively.

Table 3-2. The real-time simulation results of PSO and GA for IEEE 30 bus system with P_D = 1500 MW and P_D = 2000 MW.

Case A		P1	P2	P3	P4	P5	P6	E_{NOX}	E_{COX}	E_{SOX}	E	EC	FC	TC	t
P_D = 1500 MW	PSO	195.79	256.55	381.25	81.69	381.85	202.27	1719.67	39,626.51	9623.04	50,969.21	19,121.26	14,827.57	33,948.83	0.1326
	GA	196	255	351	79	416	203	1731.52	40,049.21	9579.83	51,360.56	19,170.74	14,835.04	34,005.78	0.4528
P_D = 2000 MW	PSO	256.32	320.57	541.95	133.1	500	248.06	2540.68	73,738.76	13,601.05	89,880.5	37,543.01	19,445.29	56,988.3	0.1227
	GA	268	287	562	127	500	256	2537.8	75,505.33	13,450.06	91,493.19	37,608.68	19,485.44	57,094.12	0.4706

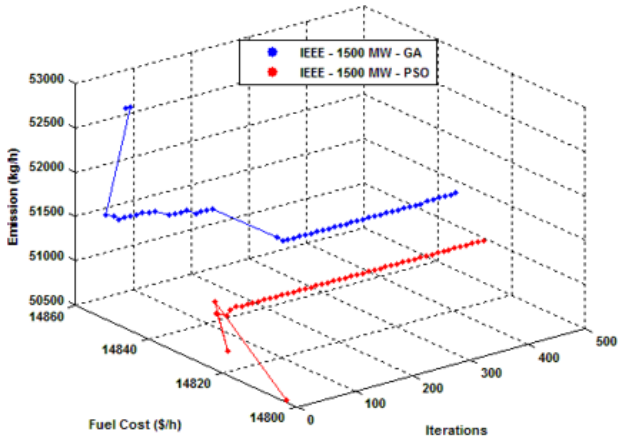


Figure 3-3. The convergence characteristics of PSO and GA with regard to fuel cost and emission for IEEE 30 bus system with P_D = 1500 MW.

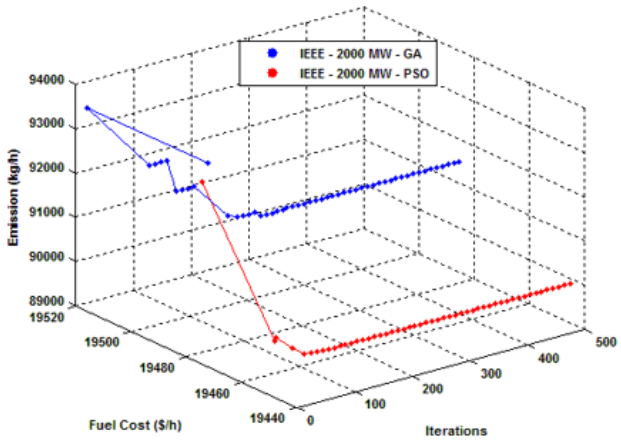


Figure 3-4. The convergence characteristics of PSO and GA with regard to fuel cost and emission for IEEE 30 bus system with P_D = 2000 MW.

3.5.2. Pakistani IPP:

This thermal power plant comprises of 15 generating units out of which 10 are multi-fuel-fired gas turbines and remaining five are steam turbines with an overall capacity of 1600 MW. The combined dispatch was performed on eight gas turbines as the remaining two are uneconomical and mostly turned off. Steam turbines take exhaust of gas turbines to operate, hence they were not considered as they do not take any direct fuel.

The data calculated and used for the dispatch of all units is given in Appendix. Transmission line losses were ignored because IPP's main concern is generation capacity which they have to produce and supply to national grid, and SO_X gas were not accounted for because of the unavailability of sufficient data. Remaining two gases (NO_X and CO_X) were considered; their penalty factors were calculated using Equation (3-4) and the procedure following this equation, for load demands of 500 and 700 MW given as:

P_D = 500 MW: h_{NOX} = 1.5751, h_{COX} = 101.1369

P_D = 700 MW: h_{NOX} = 1.7218, h_{COX} = 123.8797

The results are summarized in Table 3-3 (all powers are in MW, emissions in mg/Nm^3, costs in 10^3 \$/h, and time in seconds) while the convergence characteristics of both algorithms, with respect to both objectives (fuel cost and emission) for P_D = 500 MW and P_D = 700 MW, are shown in Figure 3-5 and Figure 3-6, respectively.

Table 3-3. The real-time simulation results of PSO and GA for Pakistani independent power plant (IPP) with P_D = 500 MW and P_D = 700 MW.

Case B		**P1**	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**E_{NOX}**	**E_{COX}**	**E**	**EC**	**FC**	**TC**	**t**
P_D = 500 MW	PSO	32.5	32.5	100	90.87	83.68	100	25	35.44	2512.49	40.04	24.23	76	117.1	193.1	0.1531
	GA	33	32.5	32	92	96	100	64	50.5	2624.22	43.32	25.32	80.82	121.6	202.42	0.8031
P_D = 700 MW	PSO	130	130	100	90.83	83.82	100	25	40.35	3093.41	48.93	29.83	108.09	158.5	266.59	0.1509
	GA	130	130	100	87	96	100	25	32	3110.72	55.41	30.05	115.1	158.4	274.4	0.5411

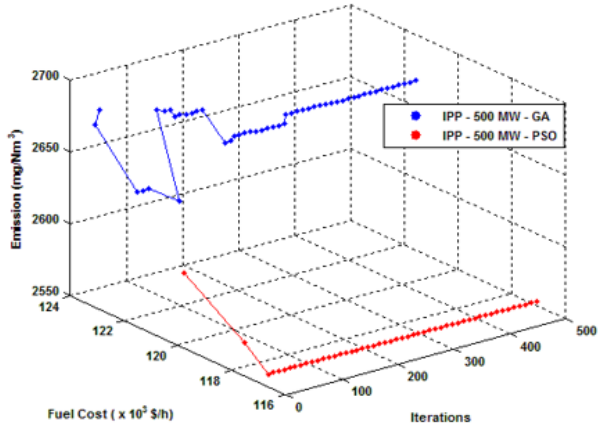


Figure 3-5. The convergence characteristics of PSO and GA with regard to fuel cost and emission for Pakistani IPP with P_D = 500 MW.

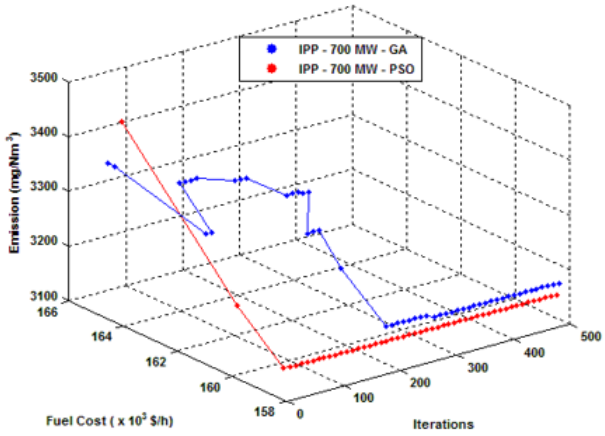


Figure 3-6. The convergence characteristics of PSO and GA with regard to fuel cost and emission for Pakistani IPP with P_D = 700 MW.

3.6. Results Discussion:

In Table 3-2, the power output of all six generators was presented as the sum of which is equal to the load demand (1500 and 2000 MW) for both algorithms (PSO and GA). Then, the emissions of all three gases (NO_X, CO_X, SO_X) from these generators were calculated and added (E) to convert into cost (EC) using penalty factor approach. The fuel cost (FC) is calculated from the generators' powers and is added to the emission cost to achieve total cost (TC) of the combined dispatch. In the end, the given

time (*t*) represents the computational time of the algorithm for that particular load demand and PSO produces the optimal solution 4 times quicker than that of GA for both load demands. Figure 3-3 shows the 3D plot of fuel cost and emission with regard to iterations for 1500 MW. It shows that PSO starts with lower fuel cost and emission, and converges quickly on the optimal solution as compared to GA which starts with higher fuel cost and emission and takes some time to converge. Figure 3-4 shows the similar 3D plot but for a load demand of 2000 MW in which PSO gets lost for a small time period in non-optimized region but quickly converges on the solution with lower fuel cost and emission, while GA converges in steps on to a solution which is not better than PSO.

Table 3-3 gives the output power of eight gas-fired generators and this total generation is equal to the load demand (500 and 700 MW) for both cases (PSO and GA). From the generators' powers, the fuel cost (FC) and emission of two gases (NO_X and CO_X) were calculated using quadratic relation of generator's output to fuel cost and emission, respectively. The emission was then totaled (E) and converted to cost (EC) by imposing penalty factor. These two costs (related to fuel and emission) were then added to get total cost (TC) of the combined dispatch of the power plant. In the end, *t* is the time taken by each algorithm to carry out the dispatch for a particular load demand. It is noteworthy that PSO is 4–7 times faster than its GA counterpart for both load demands. Figure 3-5 shows the 3D plot of fuel cost and emission with regard to iterations for 500 MW. In this figure, PSO starts with higher fuel cost but in few iteration, it converges on the optimal solution while GA remains stuck in non-optimized region. Figure 3-6 shows the similar 3D plot but for a load demand of 700 MW. In this simulation, both PSO and GA starts from nearby solutions, but then, PSO converges very quickly while GA struggles up to 300 iterations and then converges to a nearer solution of PSO, but

still, this solution is not better than the one provided by PSO.

3.7. Summary:

The combined dispatch of plant generators with respect to fuel and gas emissions was carried out using PSO and GA in MATLAB. The results demonstrate that PSO outperforms GA for the combined dispatch in terms of achieving lower fuel cost, lower emission, fast convergence, and lesser simulation time. This was validated for both IEEE 30 bus system and for an independent power plant with simulation, 3D plots, and thorough discussion. The work has successfully implemented PSO and GA algorithms for CEED of the same systems. The simulation results are compared and tabulated for different load demands. 3D plots were discussed to highlight the convergence characteristics of PSO and GA with respect to fuel cost and gas emissions. In future studies, the combined dispatch will be made more realistic, by including some other practical constraints like valve point loading, ramp rate limits, prohibited operating zones of generators, transmission line losses etc. The algorithms, PSO and GA, can be made more efficient by studying and improving their performance parameters.

CHAPTER 4: OPTIMIZATION OF HYBRID RENEWABLE ENERGY SYSTEM USING ITERATIVE FILTER SELECTION APPROACH

4.1. Introduction:

This chapter presents a hybrid renewable energy system that yields minimum total project cost and maximum reliability. The system is in modular configuration consisting of PV array, wind turbine, battery storage, AC load and a dump load. Also, the minimization of unutilized surplus power is taken into consideration as one of the design objectives. In this chapter, a new technique named iterative filter selection (IFS) approach is used in designing the hybrid photovoltaic (PV)-wind turbine (WT)-battery system to obtain the best acceptable solution while considering all the design objectives. The system is then justified by comparing with iterative-pareto-fuzzy and particle swarm optimization techniques. The technique is found to be superior in terms of total project cost with satisfaction to the load demand. The method is simulated using MATLAB and the results are presented in the chapter with proper discussion.

4.2. Hybrid renewable system configuration:

The configuration of hybrid renewable energy system used in this work is shown in Figure 4-1. The main components of the systems are wind turbine, PV array, battery storage, primary load and dump load. The PV array and wind turbine will provide energy to the system whenever there is wind or solar radiation. The energy storage device will start charging when there is an excessive energy produced and will discharge when there is deficiency in the overall power generation. There will be a limitation in charging and discharging of the storage system in order to extend the battery life. The dump load used in the system will consume the unutilized surplus power which cannot be stored by the battery. The number of WT units, WT swept area,

PV array area and number of battery units is varied in accordance to the desired total cost, reliability value and unutilized surplus power produced by each combination.

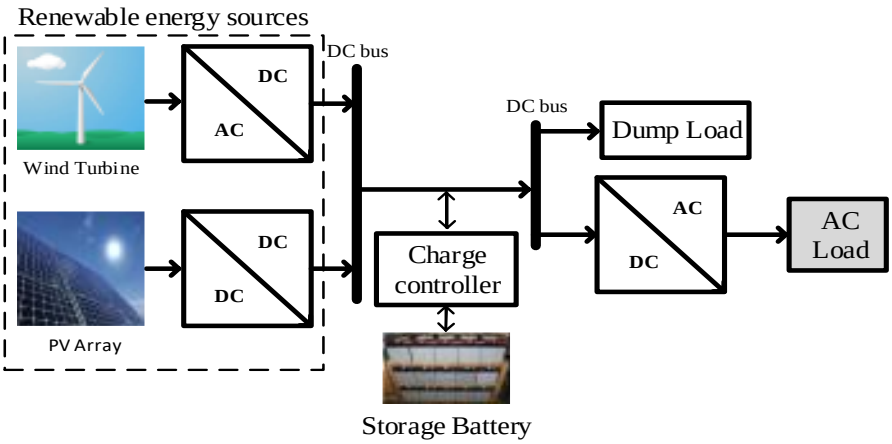


Figure 4-1. Stand-alone hybrid PV-WT-battery configuration

The data used for analyzing the system design are described as follows [30]:

The optimal sizing for WT involves the increment of swept area and thus power generated form the WT can be calculated as follows:

$$P_{WT} = P_{WTG}\left(\frac{A_{WT}}{A_{WT_{initial}}}\right) \qquad (4\text{-}1)$$

Where, P_{WTG} is the output power and A_{WT} is the new swept area for WT. However, the swept area for this system must satisfy the following condition:

$$A_{WT_{min}} \leq A_{WT} \leq A_{WT_{max}} \qquad (4\text{-}2)$$

Where $A_{WT_{min}}$ is the minimum area of the WT and $A_{WT_{max}}$is the maximum area of the WT.

The output power of PV array can be calculated as follows:

$$P_{PV} = G \times A_{PV} \times \eta_{PV} \qquad (4\text{-}3)$$

Here, η_{PV} is the module efficiency, A_{PV} is the PV array area (m^2) and G is the solar irradiance (kW/m^2). However, like WT, the area of PV array is also increased due to autonomous system and is needed to be with within the following range:

$$A_{PV_{min}} \leq A_{PV} \leq A_{PV_{max}} \quad (4\text{-}4)$$

The battery storage is used in the system to store whenever there is excess energy and discharge whenever there is deficit in energy. However, to ensure a longer battery lifetime certain conditions need to be adhered.

$$P_{bmin} \leq P_{bSOC} \leq P_{bCap} \quad (4\text{-}5)$$

Where P_{bSOC} is the state of charge (SOC); P_{bmin} is the minimum allowable SOC and P_{bCap} is the rated capacity of the battery. Also, for charging and discharging, power should not exceed the allowable hourly charging or discharging capacity which means

$$P_b \leq P_{cd\_limit} \quad (4\text{-}6)$$

Where P_b the charging or discharging power and P_{cd_limit} is the allowable hourly charging or discharging capacity.

The maximum number of batteries (N_b) has been considered for the system because from experience of the previous work [30], it was concluded that the optimum region lies within the maximum number of batteries. Also the system needs to have a dump load in order to consume the unutilized surplus power as battery cannot store beyond its limit.

The power from wind turbine is calculated by assuming its operation in the rated region ($P_{WTG} = P_R$) for the analysis duration of a year. The relevant input data used in this problem is taken from [30] where iterative-pareto-fuzzy technique is applied in while in this work, iterative filter selection approach has been used and the results have been concluded. Both methods start with generating a set of solutions but the difference lies in deciding the optimized one from these sets. The former method shortlists the non-dominated solutions and select the best one using fuzzy logic while the latter method does so by using filters designed to find the optimized solution. The filtering technique is faster and simpler to design for getting the optimized result as compared to its pareto

fuzzy counterpart. Moreover, the significance of the proposed method has been consolidated with an additional comparison to particle swarm optimization technique.

4.3. Problem formulation:

This section discusses the mathematical models applied for calculating the total cost, dump load size and reliability from [30] used in the application of iterative filter selection approach.

4.3.1. Total cost:

The total cost of the system is obtained from the following equation:

$$\mathrm{TC} = \sum_{i=PV,WT,b} I_i + OM_i - S_i + [X(t) \times Cost_{add}] \qquad (4\text{-}7)$$

Where TC is total cost; I_i is initial cost; OM_i is operation and maintenance cost; S_i is salvage value of the components; $Cost_{add}$ is additional cost on each WT and $X(t) = N_{WT} - 1$ where N_{WT} is the number of wind turbines to be considered. The initial costs are as follows:

$$I_{PV} = \alpha_{PV} A_{PV} \qquad (4\text{-}8)$$

$$I_{WT} = \alpha_{WT} A_{WT} N_{WT} \qquad (4\text{-}9)$$

$$I_b = \alpha_b \times P_{bCap} \times N_b \times \sum_{i=1}^{Yb} \left(\frac{1+v}{1+\beta}\right)^{(i-1)L_t} \qquad (4\text{-}10)$$

α_{PV} and α_{WT} are prices of PV and WT per unit area, α_b is battery price per unit kW, Y_b and L_t are life spans of battery and project respectively, v and β are average escalation and inflation rates from statistical point of view.

The present worth of the operation and maintenance cost of components in the project lifetime are obtained from the following equations:

$$OM_{PV} = \alpha_{OMPV} \times A_{PV} \times \sum_{i=1}^{Lt} \left(\frac{1+v}{1+\gamma}\right)^{i} \qquad (4\text{-}11)$$

$$OM_{WT} = \alpha_{OMWT} \times A_{WT} \times N_{WT} \times \sum_{i=1}^{Lt} \left(\frac{1+v}{1+\gamma}\right)^{i} \quad (4\text{-}12)$$

$$OM_{b} = \alpha_{OMb} \times P_{bCap} \times N_{b} \times \sum_{i=1}^{Lt} \left(\frac{1+v}{1+\gamma}\right)^{i} \quad (4\text{-}13)$$

α_{OMPV}, α_{OMWT} and α_{OMb} are yearly maintenance costs per unit area of PV, WT and battery while γ is average interest rate to consider practical statistical cost.

The present worth of the salvage value for WT and PV array can be obtained from the following equations (14) and (15). The salvage value of the battery is ignored in this study.

$$S_{PV} = \alpha_{SPV} \times A_{PV} \times \left(\frac{1+\beta}{1+\gamma}\right)^{Lt} \quad (4\text{-}14)$$

$$S_{WT} = \alpha_{SWT} \times A_{WT} \times N_{WT} \times \left(\frac{1+\beta}{1+\gamma}\right)^{Lt} \quad (4\text{-}15)$$

α_{SPV} and α_{SWT} are salvage costs of PV and WT per unit area.

4.3.2. Reliability and Dump load sizing:

In this system, the Energy Index of Reliability (EIR) is used to evaluate the quality and reliability of the system and can be measured by [30]:

$$EIR = 1 - \frac{EENS}{E_d} \quad (4\text{-}16)$$

EENS is Expected Energy Not Supplied and E_d is the load demand.

The total generated energy will be the sum of the energy obtained from PV and WT i.e. $P_g=P_{PV}+P_{WT}$ which will serve the load demand. EIR will be 100% when load is satisfied by generation and battery in case the generation alone is not ample enough to serve the load. There can be three cases possible between generation (P_g) and demand (P_d) at a given point of time:

Case1: $P_d < P_g$; excess generated power will be stored in the battery and will be dumped if it exceeds battery limits.

Case 2: $P_d = P_g$; load is satisfied by the generated power.

Case 3: $P_d > P_g$; the deficit of power will be served by the battery and the power it cannot supply will be recorded.

The reliability analysis is carried out for one year ($t = 1 \rightarrow 8760$ hours) and the above three cases will be analyzed for this duration yielding energies required for the analysis ($E = P \times t$).

4.4. Iterative filter selection approach:

In this approach, all possible solutions are generated by initializing the basic parameters i.e. PV & WT areas from minimum values and incrementing them until their maximum limits are reached. For each set of PV, WT area; objectives to be minimized i.e. cost, reliability and dump load are determined. Then, 3-filter approach is implemented based on the objectives successively narrowing down the solution set and ultimately getting the best solution. First filter is designed to deal with the critical objectives whose limits cannot be violated i.e. maximum reliability and minimum dump load. It segregates the solutions which lie within allowable range i.e. EIR $\geq$ reliability tolerance (EIR_{set}) & $P_{dump} \leq$ dump load size tolerance ($P_{dump,set}$). These values are user-defined depending on problem under consideration and serve as a guide towards the process of achieving best solution. Second filter takes into account equally following two objectives:

1. The left-over objective(s) i.e. solutions with minimum cost.
2. Random selection from filtrate of first filter to rule out the case of missing solutions with inferior cost but superior reliability and dump load size.

First half solutions are reserved for point 1 and second half for point 2 due to which this filter is named 50%-50% filter. Finally the best solution is selected by fitness function given below:

$$fitness\ function = w_1 TC + w_2 P_{dump}$$

Cost and dump load are considered in fitness function as both have to be minimized. w_1 and w_2 are weights attached with objectives; total cost and dump power respectively. If w_1 is higher, then the final solution will be inclined towards region of solutions with lower cost and if w_2 is higher, then the direction will be towards solutions with lower dump power. These weights are selected carefully as they direct the algorithm towards an optimized region depending upon the percentage of significance of the objectives to be achieved in a particular problem. In this problem, the weight for dump load is large to disregard the solutions with high dump load. The solution with minimum fitness value is the best solution of the problem.

The algorithm to optimize PV-WT-Battery system using iterative filter selection approach is given below:

1. Initialization of variables.
2. FOR Loops: $A_{PV} \rightarrow WT \rightarrow A_{WT} \rightarrow N_b \rightarrow t$
3. Calculate $P_g = P_{WT} + P_{PV}$ and check if: (a) $P_d < P_g$ or (b) $P_d = P_g$ or (c) $P_d > P_g$. Accordingly calculate EENS, P_{dump} & P_{bsoc} by checking current battery status and excess power in case (a).
4. Store and print values of P_{bsoc}, P_{dump}, EENS, EIR & TC for all solutions in respective arrays.
5. Save output in excel file.
6. First filter contains two conditions imposed on all iterations: (a) $EIR \geq EIR_{set}$ (b) $Pdump \leq P_{dump,set}$
7. Display filtered solutions obtained in step 6 in an excel file.
8. Sort these filtered solutions in ascending order with respect to cost.

9. Make a pool of n solutions from those obtained in step 8. This pool is based on 50-50% filter which is second filter in which half is top n/2 solutions of sorted array of step 8 and rest n/2 solutions are selected randomly from the same remaining array.

10. Third filter is fitness function which gives the best solution with optimal fitness value.

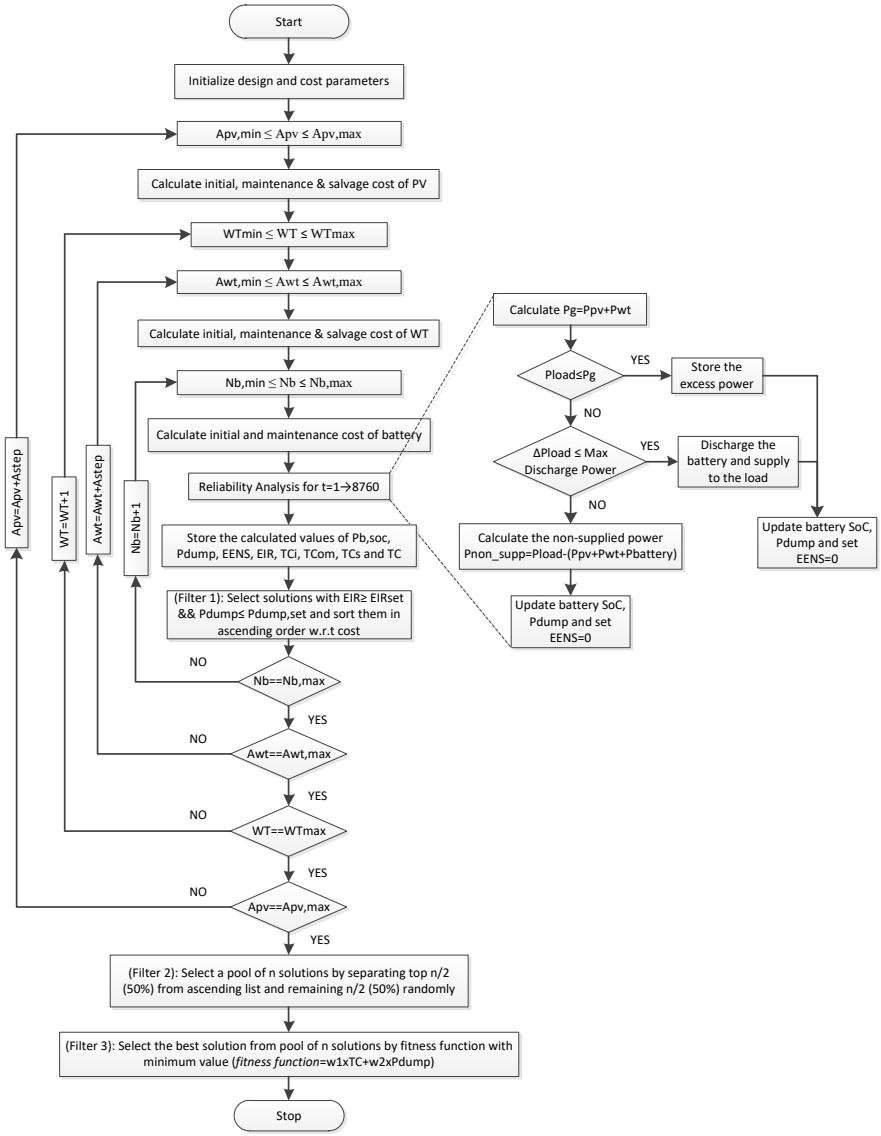


Figure 4-2. Flowchart for iterative filter selection approach applied for optimal design of hybrid renewable energy system

4.5. Results and Discussion:

The parameters for cost and reliability analysis are taken from [15] as given below:

$P_R = 4\ kW/m^2, A_{WT,min} = A_{PV,min} = 6\ m^2, A_{WT,max} = A_{PV,max} = 42\ m^2, G = 4.884\ kW/m^2/day, h_{PV} = 0.16, P_{bmin} = 0.3\ kW, P_{bcap} = 3\ kW, Cost_{add} = 0.1xTC_{WT}, N_{WT} = 2, \alpha_{PV} = 450\ \$/m^2, \alpha_{WT} = 100\ \$/m^2, \alpha_b = 100\ \$/m^2, \alpha_{OMPV} = 4.3\ \$/m^2/year, \alpha_{OMWT} = 2.5\ \$/m^2/year, \alpha_{OMb} = 10\ \$/m^2/year, \alpha_{SPV} = 45\ \$/m^2, \alpha_{SWT} = 10\ \$/m^2, N_b = 5, Y_b = 10\ years, L_t = 20\ years, \upsilon = 0.12, \beta = 0.09, \gamma = 0.12, EIR_{set} = 0.95, P_{dump,set} = 25\ kW, P_d = 10.486\ kW, T = 8760\ hr$

Figure 4-3 shows the 3D plot of the hybrid system using iterative filter selection approach. The system is designed by considering minimum total cost, maximum reiability and minimum dump load size. After the iteration process has been completed a total number of 338 possible hybrid combination is obtained shown in Figure 4-3. Among this 338 possible combinations, only 13 solutions have EIR $\geq$ 95% & $P_{dump} \leq$ 25KW. However, next step gives 10 solutions in which first half have minimum cost than the remainining solutions and second half is picked randomly from the remaining solution set. Finally, solution with optimal fitness function is the most acceptable solution.

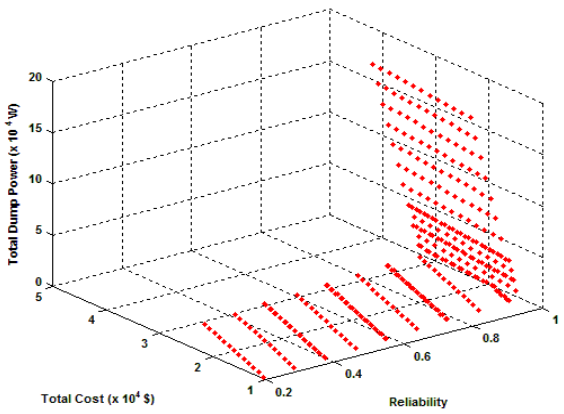


Figure 4-3. The initial iterative points using filter selection approach without the application of filters

Figure 4-4 shows the 43 pareto points obtained from total iterations of 1670 with EIR ≥ 90% in iterative-pareto-fuzzy technique from [15]. For comparison purposes, this step is equivalent to the second filter in iterative-filter-selection approach which yields 10 points from total iterations of 338 solutions with EIR ≥ 95%.

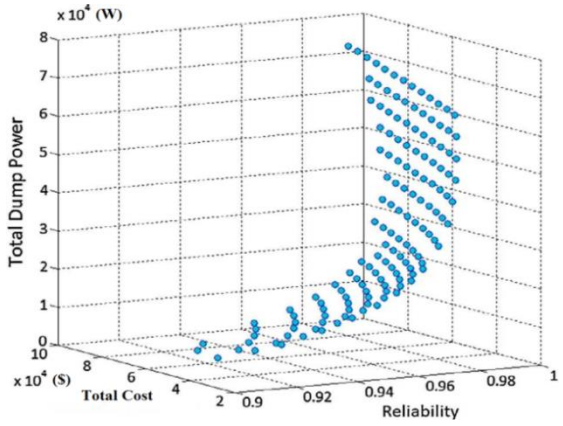


Figure 4-4. The pareto points for 90% reliability using iterative-pareto-fuzzy technique

While comparing iterative-filter-selection approach to iterative–pareto-fuzzy and particle swarm optimization (PSO) techniques, it can be observed that the proposed technique is better with huge reduction of total cost and dump power. There are three points with which these techniques can be compared with each other for this multi-objective problem i.e. total cost, reliability and dump power. Iterative filter selection approach is superior to iterative-pareto-fuzzy with respect to all objectives. In particle swarm optimization, only the reliability in the final solution is better than that of iterative filter selection approach but as whole with regards to other two objectives i.e. total cost and dump power, iterative filter selection approach is dominant over PSO. The comparison of proposed method with other two techniques is shown in Table 4-1 sealing the advantages of the proposed iterative filter selection approach.

Table 4-1. The best compromised hybrid system by iterative filter selection approach and comparison with iterative-pareto-fuzzy and particle swarm optimization techniques

No.	Parameter		Iterative-Pareto-Fuzzy Technique [15]	Iterative-Filter Selection Approach	PSO with constriction factor approach
1	Pd (hourly demand)		1.486 KW (Avg.)	10.486 KW	10.486 KW
2	EIR		90%	95%	95%
3	time		8760 hr	8760 hr	8760 hr
4	Nb		1-5	5	5
5	Method		Pareto-Fuzzy	Iterative-Filter Selection	PSO with constriction factor
6	Pwt		Cut-in/out, Pr	Pr	Pr
7	Total Solutions		Iterations: 1690 sols.	Iterations: 338 sols.	40 (20 particles for each WT no.)
8	After Filter 1		EIR: 671 sols.	EIR, Pdump: 13 sols.	*gbest:* Best solution after max.
9	After Filter 2		Pareto: 43 sols.	50-50%: 10 sols.	iterations as per PSO algorithm
		After Filter 3	Fuzzy: 1 sol.	Fitness: 1 sol.	running criterion
		WT	1	1	1
		Awt	39	30	42
		Apv	6	6	42
	3D Best Solution Details	Nb	5	5	5
10		**Pdump**	**12.80 KW**	**0 KW**	**165.39 KW**
		EIR	**96.38%**	**97.23%**	**100%**
		TC	**28380.34 $**	**14466.63 $**	**37235.88 $**
		Computational Time	**Not specified**	**1-2 s**	**1.5 - 2 s**

Finally, Table 4-2 is showing a portion of output excel file and shows the results of first 30 iterations out of 338 of iterative filter selection approach. Each iteration gives a solution to the problem. On the completion of this process, the step by step application of three filters will narrow down the feasible solutions and finally select the best compromised solution from the set. The highlighted iteration 9 is the best solution which will be extracted ultimately from these 338 iterative solutions by gradual application of filter 1 (EIR ≥ 95% & $P_{dump} \leq 25$ kW), filter 2 (50%-50%) and filter 3 (optimal fitness function).

Table 4-2. The process of determining the best possible combination for PV-WT-battery system using iterative filter selection approach

i	Apv	Ppv	WT	Awt	Pwt	Nb	Pg	Pd	Pbsoc	**Pdump**	EENS	**EIR**	**TC**
1	6	1711.354	1	6	17520	5	19231.3536	91857.36	1.5	**0**	72627.5064	**0.209345**	**11006.06792**
2	6	1711.354	1	9	26280	5	27991.3536	91857.36	1.5	**0**	63867.5064	**0.304710**	**11438.63818**
3	6	1711.354	1	12	35040	5	36751.3536	91857.36	1.5	**0**	55107.5064	**0.400075**	**11871.20845**
4	6	1711.354	1	15	43800	5	45511.3536	91857.36	1.5	**0**	46347.5064	**0.495440**	**12303.77871**
5	6	1711.354	1	18	52560	5	54271.3536	91857.36	1.5	**0**	37587.5064	**0.590806**	**12736.34898**
6	6	1711.354	1	21	61320	5	63031.3536	91857.36	1.5	**0**	28827.5064	**0.686171**	**13168.91925**
7	6	1711.354	1	24	70080	5	71791.3536	91857.36	1.5	**0**	20067.5064	**0.781536**	**13601.48951**
8	6	1711.354	1	27	78840	5	80551.3536	91857.36	1.5	**0**	11307.5064	**0.876901**	**14034.05978**
9	6	1711.354	1	30	87600	5	89311.3536	91857.36	1.5	**0**	2547.5064	**0.972267**	**14466.63004**
10	6	1711.354	1	33	96360	5	98071.3536	91857.36	15	**6198.9936**	0	**1**	**14899.20031**
11	6	1711.354	1	36	105120	5	106831.3536	91857.36	15	**14958.9936**	0	**1**	**15331.77057**
12	6	1711.354	1	39	113880	5	115591.3536	91857.36	15	**23718.9936**	0	**1**	**15764.34084**
13	6	1711.354	1	42	122640	5	124351.3536	91857.36	15	**32478.9936**	0	**1**	**16196.91111**
14	6	1711.354	2	6	35040	5	36751.3536	91857.36	1.5	**0**	55107.5064	**0.400075**	**12058.18034**
15	6	1711.354	2	9	52560	5	54271.3536	91857.36	1.5	**0**	37587.5064	**0.590806**	**13016.80682**
16	6	1711.354	2	12	70080	5	71791.3536	91857.36	1.5	**0**	20067.5064	**0.781536**	**13975.4333**
17	6	1711.354	2	15	87600	5	89311.3536	91857.36	1.5	**0**	2547.5064	**0.972267**	**14934.05978**
18	6	1711.354	2	18	105120	5	106831.3536	91857.36	15	**14958.9936**	0	**1**	**15892.68626**
19	6	1711.354	2	21	122640	5	124351.3536	91857.36	15	**32478.9936**	0	**1**	**16851.31273**
20	6	1711.354	2	24	140160	5	141871.3536	91857.36	15	**49998.9936**	0	**1**	**17809.93921**
21	6	1711.354	2	27	157680	5	159391.3536	91857.36	15	**67518.9936**	0	**1**	**18768.56569**
22	6	1711.354	2	30	175200	5	176911.3536	91857.36	15	**85038.9936**	0	**1**	**19727.19217**
23	6	1711.354	2	33	192720	5	194431.3536	91857.36	15	**102558.9936**	0	**1**	**20685.81865**
24	6	1711.354	2	36	210240	5	211951.3536	91857.36	15	**120078.9936**	0	**1**	**21644.44513**
25	6	1711.354	2	39	227760	5	229471.3536	91857.36	15	**137598.9936**	0	**1**	**22603.07161**
26	6	1711.354	2	42	245280	5	246991.3536	91857.36	15	**155118.9936**	0	**1**	**23561.69809**
27	9	2567.03	1	6	17520	5	20087.0304	91857.36	1.5	**0**	71771.8296	**0.218660**	**12535.63411**
28	9	2567.03	1	9	26280	5	28847.0304	91857.36	1.5	**0**	63011.8296	**0.314025**	**12968.20438**
29	9	2567.03	1	12	35040	5	37607.0304	91857.36	1.5	**0**	54251.8296	**0.409390**	**13400.77464**

i	Apv	Ppv	WT	Awt	Pwt	Nb	Pg	Pd	Pbsoc	**Pdump**	EENS	**EIR**	**TC**
30	9	2567.03	1	15	43800	5	46367.0304 and so on … to i = 338	91857.36	1.5	**0**	45491.8296	**0.504756**	**13833.34491**

4.6. Summary:

A new optimization method has been introduced in this work named iterative filter selection (IFS) approach for optimization problems and applied on PV-WT-Battery system. The method is compared with iterative-pareto-fuzzy and particle swarm optimization techniques and found superior in terms of system cost and dump load size satisfying higher load demand. Its computational time is also small because of its simple algorithmic structure. Some parameters like reliability tolerance and dump load size tolerance have been refined for better and fast results. Maximum number of batteries is considered only, to minimize dump load size due to which total solutions also decreased by five times compared to previous work using iterative-pareto-fuzzy technique. The best solution given by IFS approach has lowest cost, optimized reliability and no dump load for the duration of analysis.

CHAPTER 5: A NOVEL HYBRID METHODOLOGY TO SECURE GOOSE MESSAGES AGAINST CYBERATTACKS IN SMART GRIDS

5.1. Introduction:

IEC 61850 is emerging as a popular communication standard for smart grids. Standardized communication in smart grids has an unwanted consequence of higher vulnerability to cyber-attacks. Attackers exploit the standardized semantics of the communication protocols to launch different types of attacks such as false data injection (FDI) attacks. Hence, there is a need to develop a cybersecurity testbed and novel mitigation strategies to study the impact of attacks and mitigate them. This work presents a testbed and methodology to simulate FDI attacks on IEC 61850 standard compliant Generic Object-Oriented Substation Events (GOOSE) protocol using real time digital simulator (RTDS) together with open-source tools such as Snort and Wireshark. Furthermore, a novel hybrid cybersecurity solution by the name of Sequence Content Resolver is proposed to counter such attacks on the GOOSE protocol in smart grids. Utilizing the developed testbed, FDI attacks in the form of replay and masquerade attacks are launched and the impact of attacks on electrical side is studied. Finally, the proposed hybrid cybersecurity solution is implemented with the developed testbed and its effectiveness is demonstrated.

With the amalgamation of information and communication technologies (ICT) in power grids, the traditional power systems are rapidly evolving as smart grids. ICT enables remote monitoring, control, and automation of power systems [138] For interoperable operation of smart grids many communication protocols and standards are proposed for smart grids. Among them IEC 61850 has emerged as one the most popular and widely accepted standard for power utility systems [108].

Standardized communication and protocols present an increased vulnerability to

cyber-attacks. The attackers may exploit the standardized semantics to launch different types of attacks on standardized communication. IEC 61850 communication protocols are vulnerable to cyber-attacks. In literature, many attacks on generic object-oriented substation event (GOOSE) and sampled value (SV) messages are widely reported [123, 139]. Previous studies in literature showed that GOOSE messages are most vulnerable, a single contaminated GOOSE message can result in successful maloperation of circuit breakers and result in severe consequences [140, 141]. IEC 61850 standard does not present any considerations or strategies for GOOSE messages against cyberattacks. IEC 62351 standard series compliments IEC 61850 standard by providing cybersecurity considerations for different IEC 61850 messages [142].

In literature, researchers focused on developing information technology (IT) or operational technology (OT) based solutions for securing GOOSE messages against different attacks. For instance, in [143, 144] authors proposed use of Rivest–Shamir–Adleman (RSA), elliptic curve digital signature algorithm (ECDSA) and rainbow signature scheme (RSS) based digital signatures for securing GOOSE messages. However, in [143, 145] it was proved that the digital signatures result in high computational delays and hence not suitable for time critical GOOSE messages with stringent 3 ms timing requirements. Recently published IEC 62351-6 standard proposed light weight message authentication code (MAC) algorithms to secure the GOOSE messages [146-148]. Authors in [149] introduced caching-based MAC and Less-online/More-offline MAC Signatures which further reduces computational delays. Although the MAC algorithms have very less computational delays, they are symmetric algorithms which requires a pre-shared key. Safe distribution and update of pre-shared keys is a quite challenging and in turn requires a robust key distribution mechanism.

On the other hand, OT based solutions (generally outside the IT domain) for securing

GOOSE message against cyber-attacks were developed. In such solutions the contents of the communication messages are verified before they are processed further. This verification can be carried out by various methods, such as confirming the message contents received by the neighboring IEDs [150], or using machine learning tools to detect abnormal GOOSE messages [151]. In [152], authors presented a sliding window-based sequential classification mechanism to detect abnormalities. Similarly, in [153] Discrete Wavelet Transform (DWT) and Long Short-Term Memory (LSTM)-based autoencoder network is proposed to detect anomalies in GOOSE messages.

In literature, the available solutions for securing GOOSE messages are either IT based, or OT based. However, there is a need for developing holistic solutions which involve both IT and OT domains. In this regard, this work proposes a holistic solution for securing GOOSE messages using a sequence content resolver which combines both IT and OT based solutions. On IT side, the message authentication code (MAC) is checked to confirm the integrity of the received message, then a strategy based on transmission sequence counter sqNum and event update counter stNum is devised to introspect the sequence and content of GOOSE packets. On OT side, once it is confirmed that there is change in data contents based on stNum, the confirmation is acquired from the neighboring IEDs and the counterfeit messages are segregated from the real ones based on a rule based applied security. Table 5-1 presents the qualitative feature comparison of the proposed holistic solution with the existing solutions to secure GOOSE messages. The effectiveness of the proposed holistic solution is demonstrated by conducting performance evaluation tests in the real-time test bed for cyber-physical system of a standard microgrid. The main research problem is to simulate cyberattacks (FDI attacks mainly masquerade and replay attacks) on GOOSE protocol in real time digital simulator on a standard microgrid and later deploy

mitigation technique to counter these attacks. Hence, the main contributions of this work are as follows:

1. Developed real time test bed for studying cyberattack (FDI) on GOOSE protocol using RTDS and Snort.
2. Proposed novel IT+OT security scheme for securing GOOSE protocol. Snort is used to inject FDI attacks and Wireshark is used to monitor the GOOSE packets, an anti-Snort is proposed by the name of Sequence Content Resolver (SCR) which will nullify the impact of Snort and there will be cyberattack free communication between publisher and subscriber. SCR comprises of two modules i.e. COMM and ELEC, the former is the communication module which deals with the replay attacks (sequence of GOOSE packets) and the latter is the electrical module which deals with the masquerade attacks (content of GOOSE packets). Both modules together constitute SCR and mitigate the FDI attacks.
3. Demonstration of cyberattacks and proposed mitigation strategy on real time digital platform. The result of masquerade attack is presented to create a system fault alike situation on power system. The exploited GOOSE packets effect the P&C IEDs which trip the breakers or generate islanding scenario in case of microgrid, this impact is evaluated, discussed and presented.

Table 5-1. Cybersecurity solutions for securing GOOSE message

	IT		**OT / Machine Learning**	**IT+OT based deterministic**
	Authentication	Encryption		
Hussain et al. [154]	✓	×	×	×
Hong et al. [139]	×	×	✓	×
Ustun et al. [155]	×	×	✓	×
X. Wang et al. [152]	×	×	✓	×
M. Rodríguez et al. [156]	✓	✓	×	×
This work	×	×	×	✓

The rest of the chapter is organized as follows. Section 5-2 presents the background of IEC 61850 standard and control authority. Section 5-3 discusses the development of testbed and demonstration impact of cyberattacks. Section 5-4 discusses the design and implementation of the proposed holistic sequence content resolver for mitigation of cyberattacks on GOOSE messages. Finally, conclusions are presented in section 5-5.

5.2. IEC 61850 Protocols and Control Authority:

The first edition of IEC 61850 was initially developed for substation automation systems. In the later editions of IEC 61850 standard, it was extended to entire power utility automation systems. The IEC 61850 standard defines four protocols namely GOOSE, SV, MMS and SNTP:

- GOOSE for switching signals from IEDs to circuit breakers (CBs);
- SV for measurement values from merging units (MU) to IEDs;
- Manufacturing message specification (MMS) to exchange measurement readings and control commands between human-machine interface (HMI) and IEDs;
- Simple network time protocols (SNTP) for time synchronization of IEDs with GPS master clock.

An operator can trip circuit breakers via GOOSE messages during fault or maintenance. To grant access to operators at different locations and to avoid conflicts between them, a concept called control authority is used, which designates an operator's right to switch a specific circuit breaker [157]. This implementation is based on an entity called a switch object (SO), which is a combination of three logical node (LN) instances, XCBR (or XSWI), CSWI and CILO as shown in Table 5-2 and Figure 5-1. A SO takes the control parameters and an interlock logic as inputs. A particular SO can be mapped to the desired circuit switch in the simulation for control operations. A remote client can access the SO for control purposes using the MMS protocol as shown in Table 5-3. The

binding of external trip signals (published as GOOSE messages) to the corresponding circuit breaker is achieved using a generic input (GGIO LN instance), and done independently from the SO.

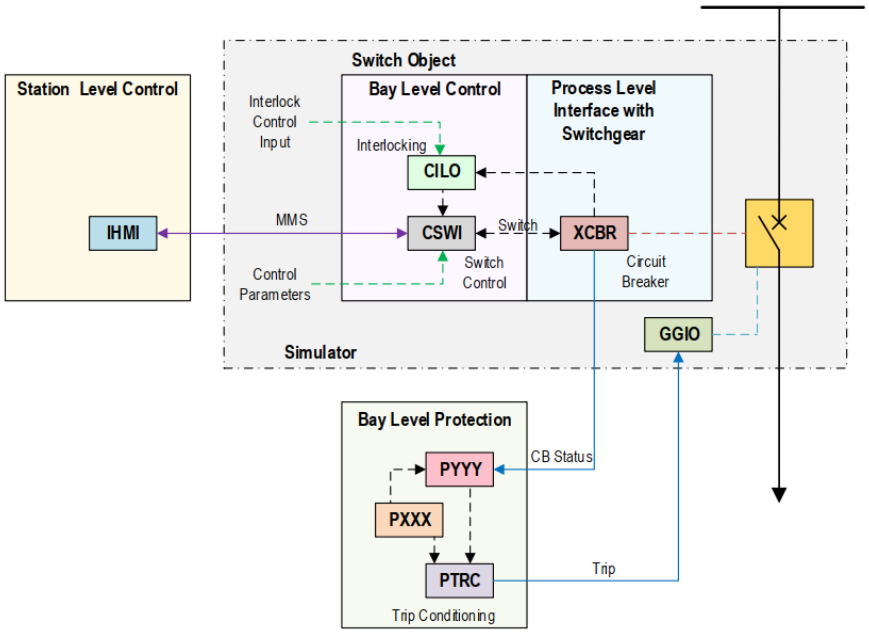


Figure 5-1. Circuit breaker control based on switch object

Table 5-2. Logical node classes and control parameters as per IEC-61850

Logical Node Class (IEC 61850-7-4)	**Description**
XCBR	Circuit Breakers - Switches with short circuit breaking capability
XSWI	Circuit Switches - Switches without short circuit breaking capability
CSWI	Switch Controller - Control all switching conditions above process level
CILO	Interlocking Function - Enable a switching operation if interlocking conditions are met
Control Parameter	**Description**
XCBR/XSWI.Loc	Represents the status of an actual switch at the process and allows taking over the manual control authority
LLNO.MltLev	Enables for more than one originator to hold control authority at the same time
CSWI.Loc	Represents the control behavior of the logical node (bay level)
CSWI.LocSta	Represents the switching authority at the station level

Table 5-3. Switchgear control based on control authority

Control Parameters				**Control Authority at each Level**			
Switch	**Bay Control**			**Manual Control**	**Originator (OrCat)**		**Category**
XCBR.Loc XSWI.Loc	**LLNO.MltLev**	**CSWI.Loc**	**CSWI.LocSta**	**Process[1]**	**Bay[2]**	**Station[3]**	**Remote[3]**
TRUE	FALSE	Not Applicable	Not Applicable	Always Allowed	Not Allowed	Not Allowed	Not Allowed
FALSE	FALSE	TRUE	Not Applicable	Always Allowed	Always Allowed	Not Allowed	Not Allowed
FALSE	FALSE	FALSE	TRUE	Always Allowed	Not Allowed	Always Allowed	Not Allowed
FALSE	FALSE	FALSE	FALSE	Always Allowed	Not Allowed	Not Allowed	Always Allowed
TRUE	TRUE	Not Applicable	Not Applicable	Always Allowed	Not Allowed	Not Allowed	Not Allowed
FALSE	TRUE	TRUE	Not Applicable	Always Allowed	Always Allowed	Not Allowed	Not Allowed
FALSE	TRUE	FALSE	TRUE	Always Allowed	Always Allowed	Always Allowed	Not Allowed
FALSE	TRUE	FALSE	FALSE	Always Allowed	Always Allowed	Always Allowed	Always Allowed

1. Current and voltage transformers (CT/VT) connected to MU
2. Switch controller communicating at process level with MU via SV and CB via GOOSE and MMS
3. Communication with switch controller via MMS

5.3. Methodology to Validate Cyberattacks:

A testbed is developed to create cyberattacks or false data injection (FDI) attacks on power systems using real time digital simulator (RTDS) and it can be further utilized to investigate the attacks on IEC-61850 communication protocols and to analyse its impact on power systems.

5.3.1. Testbed for implementation and modification of IEC 61850 communication

The time stringent communication protocols in IEC-61850 are GOOSE and SV, first one is responsible to send control commands from protection and control (P&C) IEDs to circuit breakers (CBs) IEDs while the latter provides sampled and digitalized values of current and voltage measurements to the same P&C IEDs from merging units (MU). Hence, both these control commands and measurements data being transferred by GOOSE and SV protocol respectively fall under the protection scheme of substations where timely measures are necessary. An attacker who can exploit the vulnerabilities of these protocols can do great damage both to power equipment and supply being fed to consumers. The modification in SV packets lead P&C IEDs to receive fake data and they directly or on the approval of operator under false pretences, can issue wrong commands to associated CBs. In addition to this indirect attack via SV to change the status of the CB, the attacker can also directly control GOOSE packets to trip/reclose CBs of his choice to demonstrate a picture of fear, havoc and economic turmoil among the working personnel and connected customers. The explained attack is conducted in following two steps:

1) Real time simulation of GOOSE packets between IEDs,
2) Fake data is fed to IEDs through the GOOSE protocol, simulating a compromised IED accessed and controlled by an attacker.

The implementation is carried out using an interconnection system of RTDS [158], Wireshark [159] and Snort [160] as shown in Figure 5-2. The first system provides real time simulation features for any power system to be studied. Its recent network interface card GTNETx2 is the communication interface for simulation of communication packets coming out and going into the simulated power system. Each GTNETx2 card has two modules, and each can simulate one protocol at a time such as GOOSE, SV, MMS, DNP3 etc. The setup to test and modify the simulation of communication packets is through a publisher-subscriber setup where transmission is broadcasted in multicast fashion by the publisher and different subscribers can subscribe to the data being transmitted. Due to multicast nature of GOOSE packets, an attacker who gets access to the substation's network can view the GOOSE packets and also inject counterfeit GOOSE messages with faulty information. This action may lead to tripping or holding the circuit breakers which damages the equipment causing harm to the stable operation of power system. The GOOSE messages being published and later being subscribed by particular IEDs are monitored by an open-source tool Wireshark. For modifying the packets, Snort, another open source tool, with some changes is being utilized to capture the packets from publisher, modify them and later inject them in to the network. Snort basically captures the GOOSE packets published by P&C IEDs and modifies them by changing the value of stNum field to high number and value of data field as selected by the user. These modified packets are then re-published by Snort which are received by the CB IEDs. The testbed has the advantage that it is based on open-source tools. It is capable of simulating and modifying the communication packets of various protocols such as GOOSE, SV etc. which constitute an attack and is later supporting in evaluating the impact of modification in communication packets over the automated power system.

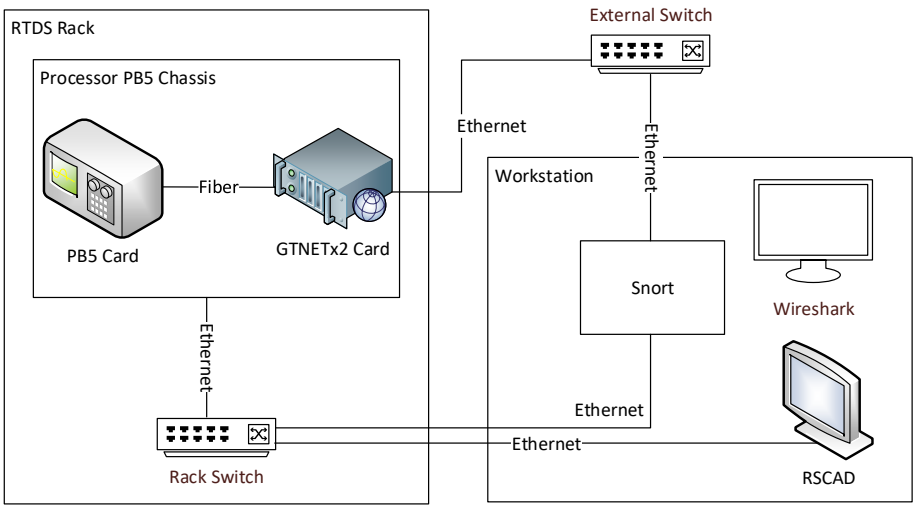


Figure 5-2. Testbed with RTDS, Snort, and Wireshark.

5.3.2. Simulation and modification of GOOSE packets

GOOSE protection is the most critical protocol as it is used in protection schemes to trip/reclose CBs in response time matching within 3 ms. In order to simulate the GOOSE packets between publisher-subscriber setup, both modules of a GTNETx2 card are engaged; one acting as sender or publisher while the other is behaving as receiver or subscriber. The communication packets in between them are of 4 different data types (integer, binary, two-bits and floating point) out of which the tripping/reclosing command is usually sent with boolean type of data. As shown in Figure 5-3, IED 1 is sending the 4 types of data [3 0 1 60] and same is subscribed by IED 2 while IED 2's broadcasted data [5 1 3 100] is being subscribed by IED 1. The attack is simulated in Figure 5-4 when IED 1 is acting as publisher with data [3 0 1 60] which is being lost and modified because IED 2 is receiving counterfeit data [9 1 3 22.22]. This modification is conducted by capturing the publisher packets using Snort with GOOSE packets important parameters i.e. control block (gocbRef) and data set (datSet). The packets are monitored on Wireshark and this experiment validates the direct FDI attack on GOOSE communication between IEDs and its impact on electrical side is very

harmful. For instance, an attacker can corrupt the boolean value in order to open circuit breakers for cascaded tripping affecting consumers or he can also keep the breakers in closed position during actual system fault to damage the equipment.

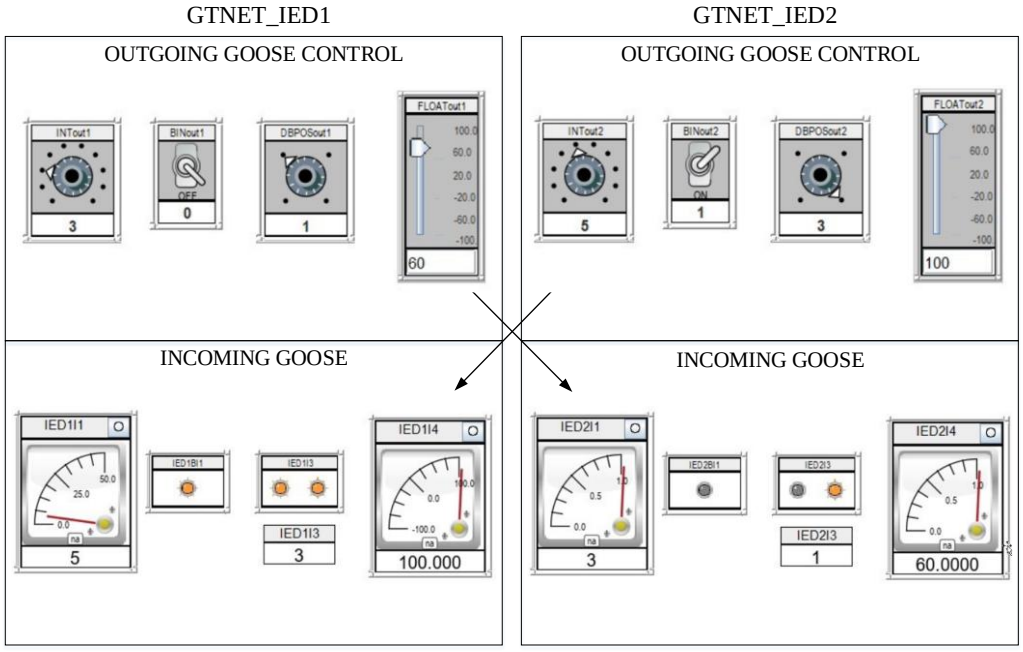


Figure 5-3. RTDS runtime for GOOSE communication between IED 1 and IED 2 before the manipulation of packets by the attacker

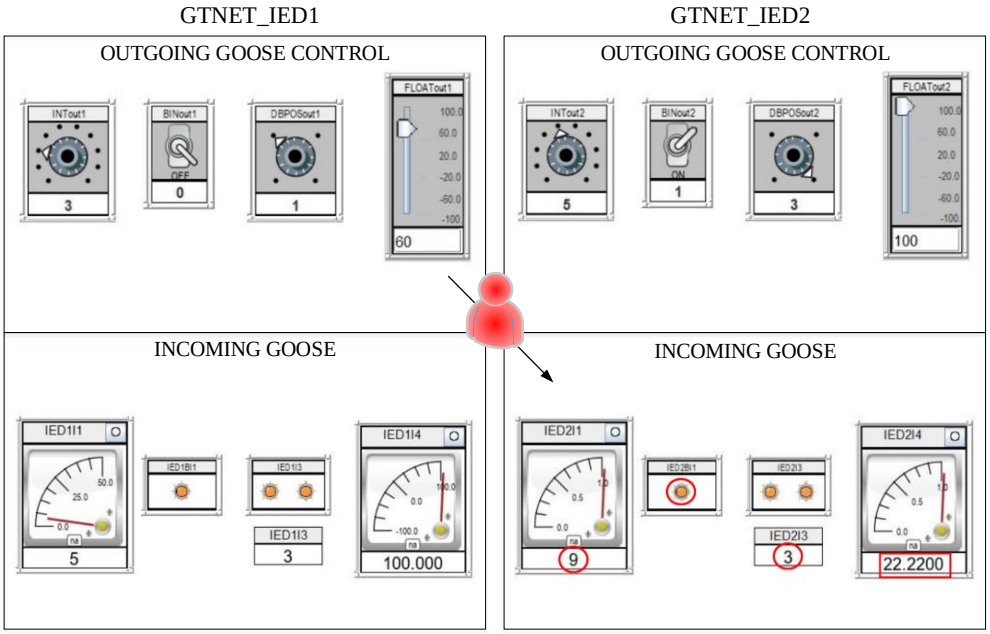


Figure 5-4. RTDS runtime for GOOSE communication between IED 1 and IED 2 after the manipulation of packets by the attacker

The original GOOSE packet and the corresponding modified packet as observed in Wireshark is shown in Figure 5-5. The modification is done by the attacker in all 4 data types and IED 2 is receiving the counterfeit message [9 1 3 22.22] instead of originally broadcasted message [3 0 1 60] by IED 1 as publisher. The packets are focused on the integer and boolean data types only as the boolean data is normally used to change the status of the breaker. The two counters i.e. status (stNum) and sequence (sqNum) in GOOSE packets are to be carefully observed from security perspective because the first status counter increments on every new event or status change while the latter sequence counter increments on periodic transmission of repetitive packets. sqNum keeps on increasing its value by 1 until its maximum value is reached while stNum will stay as it is and will only change once there is any new event meaning once there is any change in the data items of GOOSE packets. The original and counterfeit messages can be compared in parallel using their timestamps as the genuine packet originated from

GTNETx2 card has older timestamp of year 2004 which can be synchronized to present date and time but for identification purposes of original GOOSE packets, the time and date are not synchronized. The timestamp of fake packet is aligned with the time of experiment i.e. year 2020 as per the workstation's clock with Snort installation used for modification of packets.

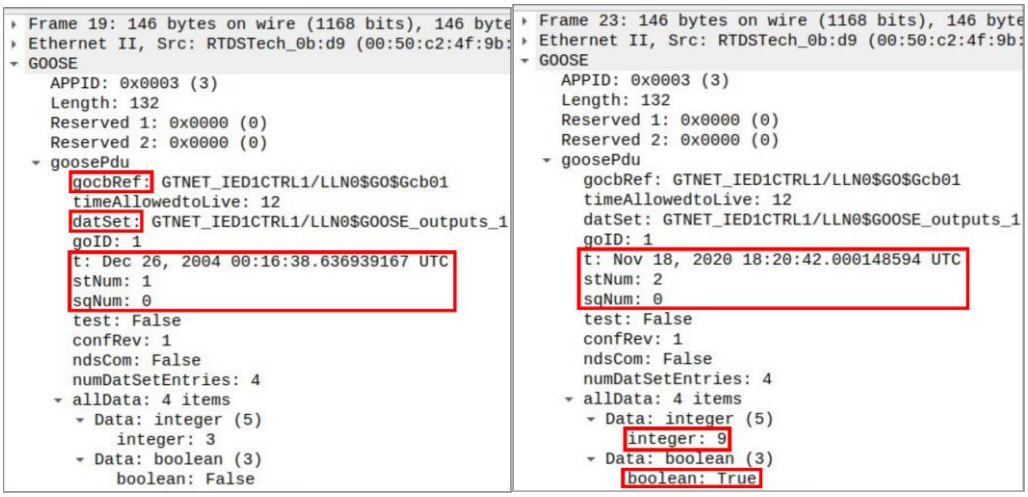


Figure 5-5. Original and counterfeit GOOSE packets for IED 1 on LAN port

The GOOSE protocol is the critical one among others in IEC-61850 power system automation standard due to its role in protection schemes of electrical network, hence suitable countermeasures should be devised based on the concepts of cyber and physical domains to secure power system communication [50].

5.3.3. Impact of FDI attacks on Simple and Complex Electrical Systems

In a doubly fed system with 3 buses as shown in Figure 5-6; bus 1 and 2 has a circuit breaker CB1 in the middle and there is resistive load connected to bus 2 while bus 3 is connected directly to bus 2 with line impedance. The bus 1 and 3 are source buses. The GOOSE packets can send tripping/reclosing command to CB1 and its impact is evaluated on electrical side. Normally, the circuit breaker is closed but to disturb the system, a GOOSE tripping command can be sent as discussed before by changing the

data item of the Boolean type to TRUE. This will cut off Source 1 on the left side and Source 2 on the right side will be the only one remaining now feeding the resistive load at bus 2. The redundancy of dual source has been compromised, the breaker current will drop to near zero while the condition of bus voltages before and after tripping is given in Table 5-4.

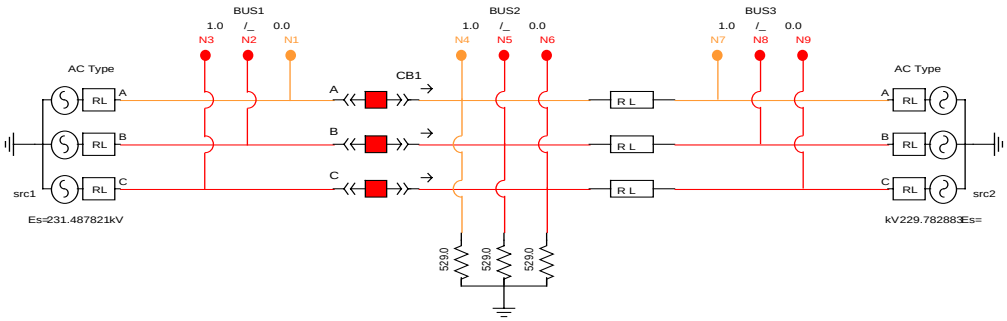


Figure 5-6. 3-phase doubly fed system in RSCAD Draft with 3 buses, circuit breaker, isolators and load

Table 5-4. Voltage before and after tripping on source and load buses

Parameters	Source bus 1	Load bus 2	Source bus 3
Voltage pre-tripping	230 kV	229.9 kV	230 kV
Voltage post-tripping	231.5 kV	226.8 kV	228.7 kV

This impact on a simple electrical system creates disturbance and stability issue once the circuit breakers are controlled by counterfeit GOOSE commands. The effect becomes manifold as the circuit becomes large and complex. The GOOSE packets have been simulated and modified and now its impact on a standard electrical system known as Banshee microgrid will be discussed as shown in Figure 5-7 [161].

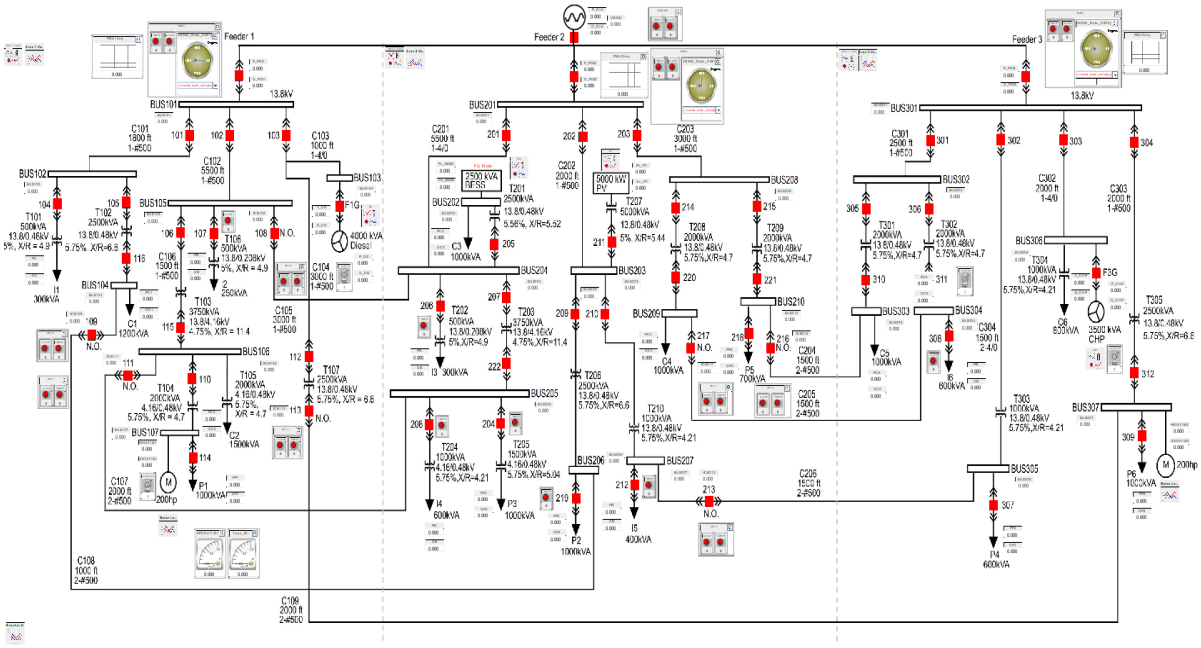


Figure 5-7. Runtime single line diagram of Banshee microgrid

Banshee microgrid, a commonly used system in real time simulation studies, includes three radial feeders connected to the grid that feed three independent areas. The independent areas can work autonomously in islanding mode but can also be inter-connected through normally opened (N.O.) tie switches. Switching between grid-connected and islanding mode simply requires to trip the main breaker of the area. This can be achieved for example by sending a simple GOOSE packet with boolean data set to 1 that triggers the islanding mode. When entering islanding mode, the frequency drops. If the generation in the independent area, now isolated from the grid, is insufficient to satisfy the load demand in isolated area, further tripping or load shedding may follow. Isolating power components by tripping specific breakers in different areas, eventually leads to disturbances in the overall system.

Regarding the generation assets, the Banshee microgrid includes:

- In the first area, a 4 MVA diesel that implements the governor, exciter and synchronous generator model.

- In the second area, a 5 MVA photovoltaic (PV) with 2.5 MVA battery energy storage system (BESS) based on the average value model for converter.
- In the last area, a 3.5 MVA natural gas fired combined heat and power (CHP) that implements the same governor, exciter and synchronous generator model used in area 1. The system further includes the following components:
- Transformers: with primary voltage level of 13.8 kV stepping down to 4.16 kV, 480 V and 208 V secondary voltage levels.
- Loads: Dynamic aggregated ones (categorized into critical, priority and interruptible) and motor loads (induction motor driving 200 horsepower (hp) chiller compressor).
- Cables: modelled with series resistance-inductance (RL) impedances.
- Circuit breakers: including synchro-check capability for main incomers (3 areas) used to connect each area to the grid. All these breakers including in each area can be controlled by external trip/reclose signals or manual push buttons in Runtime of RSCAD.

Due to its design, the Banshee microgrid is a great fit to investigate islanding scenarios. In such scenario, an area is islanded to make sure that its frequency would remain stable, and that generation can keep up with the demand in the area at least. In case of the frequency drops, each area has controls in place to prioritize some loads and shed them if needed. Islanding also modifies the generation assets operating points; for instance, BESS in area 2 shifts from PQ to VF mode. Figure 5-8 shows the difference in steps 1 to 5 observed after islanding between areas with renewable generation (area 2) and areas with conventional generation (areas 1 and 3). After islanding an area by tripping the main incomer breaker, the frequency drops below the nominal frequency and the area has not enough generation capacity to reach nominal frequency back. Thus

interruptible loads are shed, such as I2 in area 1. Furthermore, the sources change to new operating points and finally the rotating phasors at the top of each diagram indicate the discrepancy of voltage frequency between the grid and the area. In area 2, the situation is more favourable as the battery provides power to the area allowing it to avoid tripping interruptible loads such as I3 in area 2.

Beyond real time islanding scenarios, the Banshee microgrid provides the opportunity for power system studies for many electrical systems cyberattacks. For instance, an attacker injecting false data between the Aggregator (an equipment responsible for communication with distributed energy resources (DERs) and optimization to provide economical energy from them) and DERs could prioritize specific DERs thus creating monopoly for selling electricity or corrupt load shedding controls. Denial of Service (DoS) attack can also efficiently target one of the Aggregator to block available power information from DERs, resulting in generation assets to overload for long time, leading to their damage or failure.

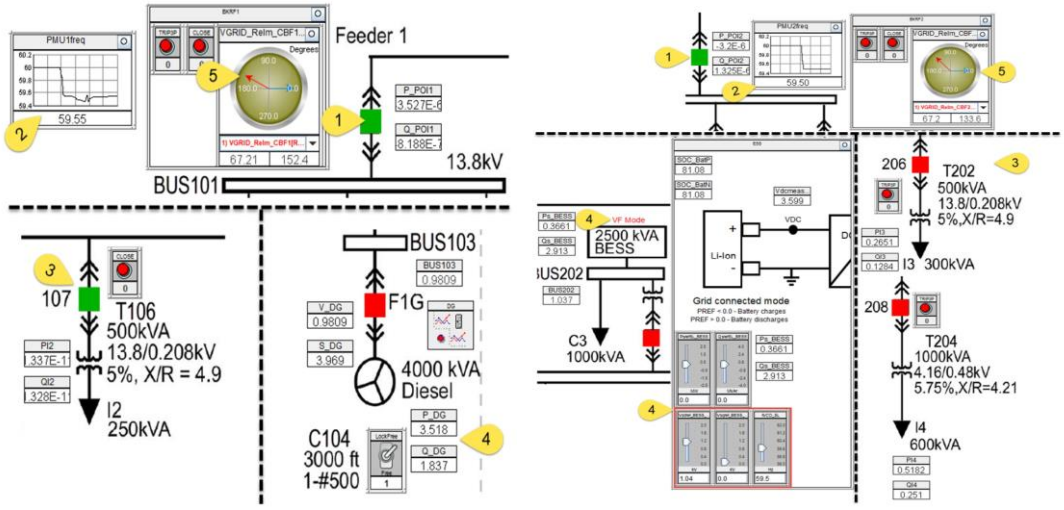


Figure 5-8. Islanding Area 1 or Area 3 vs. Area 2

5.4. Implementation of Hybrid Solution:

In this work, a hybrid solution is proposed that functions on knowledge of cyber and physical domains of the power system. ICT-based solutions may present a high false negative/positive ratio and cannot do much protection once the attacker breaches the electronic boundary of substations. Hence, holistic countermeasures based upon communication and power fields provide enhance security towards the cyberattacks. The communication packets and protocols as defined in IEC-61850 for power system communication consists of header and payload. An attacker tries to exploit either or both in order to launch replay and masquerade attacks. Hence, the proposed solution tackles both sequence and content of the packets and handles them to rule out traces of exploitation in terms of false data injection.

The sequence will be checked by the first module based on communication concepts, and the content will then be investigated by the second module based on electrical concepts. For GOOSE communication packets, the sequence can be checked by analyzing the status and sequence counters (stNum and sqNum). The replay attacks can be detected and mitigated if these counters contain older values compared to the previously stored packet. In addition, timestamps can be additionally used to check in the case if the attacker has replayed an older packet instead of creating a new one with new values of the counters. For content exploitation, the electrical understanding of the data items in GOOSE packets have to be addressed. As the data items contain mostly binary values representing the tripping/reclosing status of circuit breakers, hence a method have to be devised or adopted to get a valid confirmation of such requests coming from protection and control (P&C) IEDs to the CB IEDs. In [150], they have developed a scheme to check changes in relay settings and sensor measurements and controlling directly CB IEDs by electrical based mathematical equations and

calculations. Based on these calculations, they check the behavior of other IEDs in the vicinity compared to the target IED and await their approval to honor or dismiss such requests, resulting in changing the breaker status. The block diagram of the mitigation strategy is shown in Figure 5-9. In addition to this strategy and to make our solution effective, the use of MAC algorithms on communication level is also applied to authenticate the data and source of communication packets [156]. The publisher IED appends the GOOSE message with MAC value generated using the secret pre-shared key and sends it to the subscriber. The subscriber IED receives both the GOOSE message and MAC value. Then subscriber recalculates the MAC value for the received GOOSE message using the secret pre-shared key and compares this calculated MAC value with the received MAC value. If the MAC values do not match, the packet is rejected.

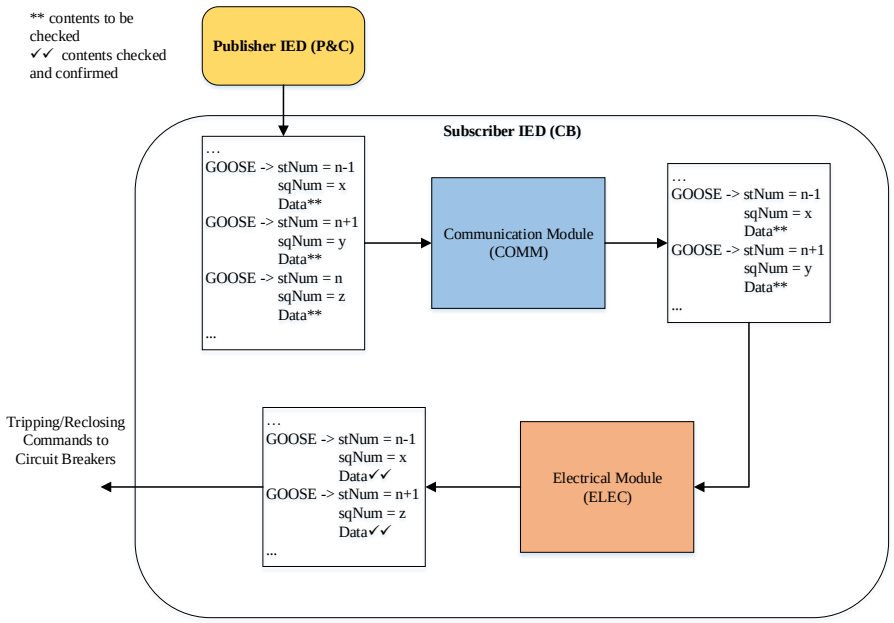


Figure 5-9. Block diagram of Sequence Content Resolver (hybrid solution)

The sequence module in the sequence content resolver will check stNum and sqNum to decide whether it is a replay attack or not, while the content module will rule out masquerade attack by cross-validating the commands with neighboring IEDs. The try

to falsely open or close circuit breakers can be via different paths as described in an attack tree as shown in Figure 5-10 [150]. The access to the substation network can be from inside the substation (process bus) or remotely from outside (station bus). Afterward, an attacker would try to access HMI, relays settings, control commands, and sensor measurements either individually or in combination, all of this in an attempt to trip or reclose circuit breakers. The intended impact is to trip circuit breakers, transmission lines, bus bars, transformers, and other critical infrastructure providing either supply to consumers or protection to the infrastructure. The objective is to create a havoc in the working personnel and the connected consumers in order to create an economic turmoil.

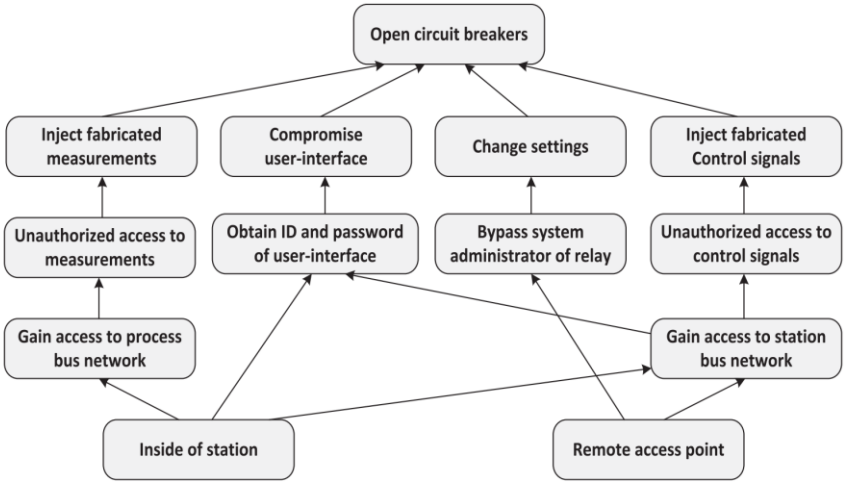


Figure 5-10. Attack tree showing the paths for potential cyberattacks [150].

Mainly, three types of exploitations are attempted by an attacker [150] to disrupt the operations of circuit breakers. The first one is to change the configuration settings of relays. The second is to inject false data into measurement sensors. The third is to directly control the circuit breakers to affect the connected consumers for malicious objectives. The first two exploitations are indirect and lead to tripping/reclosing of circuit breakers, while the third one is the direct attempt to change breaker status by issuing counterfeit messages. In [150], they have successfully developed the method to

counter-check the control commands with surrounding IEDs. Only after their approval will allow or block tripping/reclosing signals be put through. Our content module has adopted the physical or power domain-based mitigation methods from [5]. The content of GOOSE packets is verified by those techniques, resulting in passing the genuine commands and blocking the ones originating from an attacker. The difference in our work compared to [5] is that a holistic cyber-physical solution have been provided at the subscriber IED level. The cyberattack will be fought on both levels of communication and power domains by the proposed novel sequence content resolver.

Figure 5-11 shows the functional diagram of the novel sequence content resolver. The publisher or P&C IED can be accessed directly from the substation network by process or station bus in order to change the status of circuit breakers. The indirect access would be to again open/close the circuit breakers by changing the settings of relays or sensor measurements such as current/voltage transformers and merging units. The control commands are sent by P&C IEDs to CB IEDs and the previous packets (Z) are stored in order to communicate privately in case of attack on channel between the publisher and subscriber IED and later they help too to diagnose the attack on publisher IED. Once the packets are received by subscriber IED over LAN, their previous counterparts (Y) are stored, and the present packets (X) are submitted to the communication module (COMM), which will check the sequence of packets based on stNum and sqNum counters. The function of this module is to look out for replay attacks by issuing a proper alert. For replay attacks, the stNum and sqNum of present packets are compared with that of their previous counterparts, if they are older, then the packet is discarded with an alarm of replay attack. Otherwise, the packets are passed to the electrical module (ELEC) for investigation of masquerade attacks or content exploitation. The increment in stNum is analyzed with the help of neighboring IEDs in order to

differentiate between real and fake commands. After getting approval from surrounding IEDs, the real commands are passed while fake commands are alarmed as masquerade attacks. Afterward, only the data items of the packets with their past counterparts both in publisher and subscriber IEDs are checked step by step to find and declare attacks on sender and channel, respectively. Further description on the working of both modules is given below:

5.4.1. Sequence or Communication Module (COMM):

This module checks for the exploitation in the sequence in the form of replay attacks. First, the MAC value is calculated for the received message using the pre-shared secret key and compared with the received MAC value. If the MAC value does not match the packet, it is discarded, otherwise the packet is processed further. If the value of sqNum is lesser than that of the previous packet or the timestamp is two minutes older [156], it means that the attacker is replaying an old packet, and it should be discarded. The same thing is done for a packet with older stNum but if the value of stNum is greater than that of its previous packet, it can be either a genuine status change or a masquerade attack by the attacker. It also signals that the data items of the GOOSE packet are now different than that of the previous packet, and hence it should be analyzed by the content module.

5.4.2. Content or Electrical Module (ELEC):

In this module, the packets are investigated for masquerade attacks where the contents of the packets are definitely changed by the attacker. The change is signified by increased stNum, but now the module will take surrounding IEDs into confidence for confirmation of this command signal. The IEDs are approached by calculating different parameters depending upon the case of exploitation, as explained in [150], and the same

is adopted in this work. For a change in relay settings or sensor measurements, they indirectly impact the associated control commands of circuit breakers and hence should be verified by the neighboring IEDs before executing it. The direct attack on circuit breaker control via the GOOSE command is also possible and can be carried out by the attacker. The following parameters and calculations in time less than operational protection scheme is investigated for target IED by communicating the neighboring IEDs [150]:

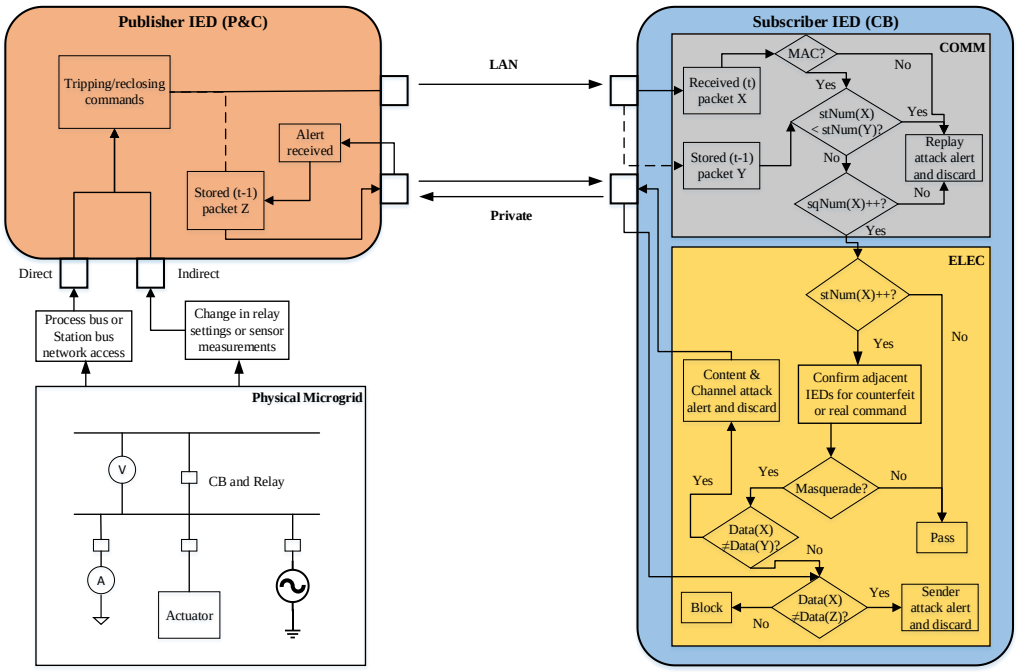


Figure 5-11. Functional diagram of novel sequence content resolver for GOOSE communication packets.

1) For a change in relay settings, if there is no loss of protection coordination scheme, the adjacent IEDs will permit control command; otherwise, it will be blocked.
2) For a change in sensor measurements, the fault transients of neighboring nodes will be compared, and the decision to permit or block the control command by the target IED will be taken.
3) For direct circuit breaker control attack on IED, the security gateway will respond if there is an impact with respect to line overloading and bus voltage conditions. If

the impact is potential cascaded tripping of lines or voltage stability issue, then the blocking signal will be sent by the security gateway to the IED under consideration. After the installation of sequence content resolver at subscriber IED level, the genuine packets are streamlined in contrast to section 5.4.2 and Figure 5-5. The counterfeit messages which were sent by the attacker with incremented stNum and changed data items are discarded while the real and genuine packets are passed with the same stNum and incremented sqNum as shown in Figure 5-12. Further from the comparison of fixed timestamps, it is also clear that both packets are originated from the network interface card of RTDS. Therefore, both timestamps are the same representing the same fact, and are set so for easy identification of genuine packets, while fake messages contain the timestamps of the workstation from where they are originated. Moreover, the stNum will be incremented in case of any new event or status change in case of fault or maintenance and that will be passed with the approval of neighboring IEDs. Otherwise, the stNum will remain the same (1 to 1), and sqNum will be only incremented (0 to 1) to show the transmission sequence of packets. Any modification in the contents of packets in the name of a new event (incremented stNum) will be flagged and discarded or blocked on the spot.

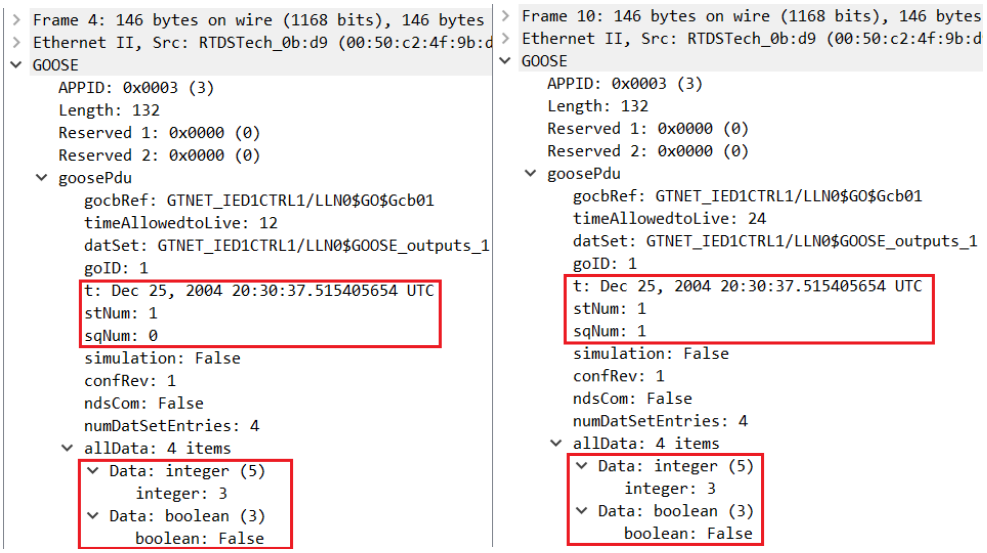


Figure 5-12. Original GOOSE packets for IED 1 on LAN port with sequence content resolver

5.5. Summary:

In this work, a methodology to validate cyberattacks and evaluate their impact on power systems is established with the help of a testbed focusing on GOOSE, the most critical protocol utilized for implementing protection. The protocol has been implemented, and modified GOOSE messages have been sent to a simulated electrical system in order to observe its impact. This allowed us to investigate the electrical effects and discuss broad categories of countermeasures. A holistic cybersecurity solution named as Sequence Content resolver is also proposed and implemented using the same test bed. Future work will make the solution more robust and explore other IEC-61850 based communication protocols for vulnerabilities such as SV and MMS. Further, advanced mitigation methods will be developed to secure devices and communication inside automated power systems while fulfilling the strict performance requirements for these environments.

CHAPTER 6: AMELIORATION OF CYBERATTACKS ON SAMPLED VALUES IN AUTOMATED POWER SYSTEMS USING A NOVEL SEQUENCE CONTENT RESOLVER

6.1. Introduction:

This work deals with cyberattacks on Sampled Value (SV) protocol in terms of false data injection (FDI) to launch replay and masquerade attacks in order to cripple the protection and control intelligent electronic devices in the light of power system automation standard IEC-61850. The SV packets are simulated, modified and mitigated in real time and the impact on a standard power system is evaluated. After implementing and analyzing the exploitation of SV communication by the attackers between publisher and subscriber setup, a novel cybersecurity solution named sequence-content resolver is proposed, designed and implemented. It is a light-weight method based upon the communication and electrical aspects of the protocol in consideration and is intended for time critical protocols such as Generic Object-Oriented Substation Events (GOOSE) and SV. It is a holistic information technology (IT) and operational (OT) based solution to provide required results by protecting the power grid from FDI attacks on automation protocols with time stringent requirements.

Nowadays power systems are evolving into automated smart grids with integration of advanced information communication technology (ICT) [162]. This automation provides the convenience of remote monitoring and control to power system operators [163]. To enhance this functionality and include interoperability of devices from different vendors in the power industry, substations and power grid have developed consensus on a universal automation standard, IEC-61850 [108]. This standard gives guidelines on the modelling of devices in an electrical system as a logical environment and communication between them through different protocols. The communication

protocols define the structure and time requirements over communication layers based on the end devices. The most significant protocols in the IEC 61850 standard responsible to carry out the communication in power system are GOOSE, SV, Manufacturing Message Specification (MMS) and Simple Network Time Protocol (SNTP). The former two protocols are time critical and are used to transfer messages between protection and control (P&C) intelligent electronic devices (IEDs) and circuit breakers (CBs) IEDs via GOOSE / merging units (MUs) IEDs via SV. The current and voltage values collected by current transformers (CTs) and potential transformers (PTs) across different points in the power system are gathered by MUs and transferred to related protection and control (P&C) IEDs as sampled values via SV protocol. P&C IEDs send tripping/reclosing commands to circuit breakers, based on these sampled values by following GOOSE protocol. The MMS protocol is used to communicate between human machine interfaces (HMIs) and IEDs while the SNTP protocol is used for time synchronization of devices and events to GPS clock.

The communication protocols defined in IEC 61850 function over different communication layers of the OSI model so that the packets can reach the target destinations in required time. The critical device for attack in the power system are the P&C IEDs together with their associated communication [164]. The engineering workplace in control centres may have access to internet, which opens an access for adversaries to infiltrate and gain foothold in power system communication network [165, 166]. Now, an attacker who has gained access to substation network can directly access the IEDs on substation LAN. In this regard, GOOSE and SV protocols are primary target for the attackers. With the former, attackers can directly control the protection devices in the field [141, 167]; whereas with the latter, they can indirectly lead the IEDs to achieve the same objective as shown in Figure 6-1. The SV protocol

is used to send sampled measured values of currents and voltages. If these values are tampered with and matched with fault conditions by the attacker, the IEDs will respond to the non-existent fault created in the form of cyberattack. The MMS protocol is time-relaxed compared to the GOOSE and SV protocols, and it communicates HMIs with the IEDs while SNTP is responsible for maintaining accurate time stamping of events performed by various devices in the power system. Hence, in automated communication inside power grid in the light of widely accepted IEC 61850 standard, it is of paramount importance to develop algorithms and smart solutions which can fend off and mitigate attacks from the cyber space on both the devices and the communication.

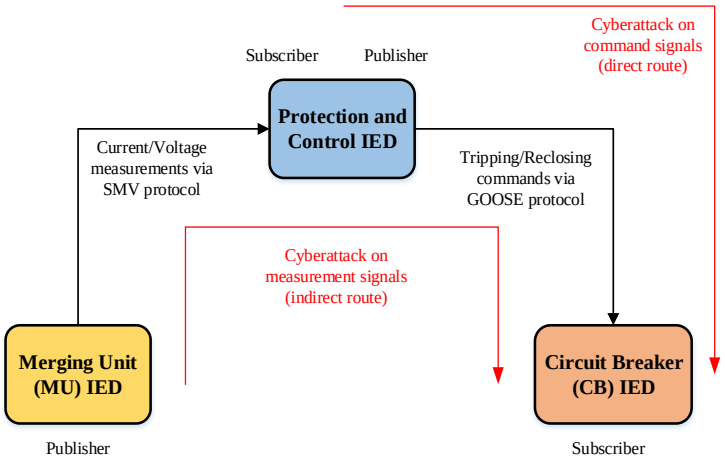


Figure 6-1. FDI attack on P&C IED (direct route via GOOSE) and on MU IED (indirect route via SV).

The Intruder Detection Systems (IDSs) implemented in reported literature are signature based, specification based and anomaly based [143, 168, 169]. Signature based systems identify attacks with the help of database containing attack samples and are not much explored. In specification-based methods, deviations from the defined rules and syntax in the packets results in the classification of attacks. They are mostly applied category in the cybersecurity domain, but it is difficult to generalize them as

the different rules have to be specified for each protocol. Anomaly detection methods work by analyzing the network traffic and the abnormal behavior in the traffic are used to profile the attacks. The attacks can be of various types such as replay, false data injection (FDI), denial of service (DoS) and masquerade. Among these types, masquerade attack is the difficult one to detect and mostly the applied security systems rely on detection of attacks only. The added protection namely intruder detection and prevention systems (IDPS) are rarely addressed and deployed in real environment.

IEC 62351 standard complement the IEC 61850 standard by proving the cybersecurity strategies to protect the IEC 61850 communication messages [142]. The IEC 62351 security solutions involve different authentication and encryption algorithms to secure the channel between client/server and/or publisher/subscriber [156, 170]. Different IT methods are applied in current literature including IEC-62351 recommended algorithms to secure SV messages. Hence, different hash-based message authentication code (HMAC) can be employed as prescribed in IEC 62351-6 such as Secure Hash Algorithm-256 (SHA-256) and Advanced Encryption Standard (AES) Galois Message Authentication Code (AES-GMAC) both of which ensure the delivery time of stringent time requirement protocols such as 3 ms in case of GOOSE and SV using symmetric key cryptography (secret key sharing is required at both ends of communication). The Message Authentication Code (MAC) algorithms viz. SHA-256 and GMAC provides authenticity of message while encryption to retain confidentially of message content is carried out by AES and AES Galois/Counter Mode (AES-GCM). The application of MAC algorithms is already attempted successfully in works of [170] and [156] and is hence not much focused in this work. In addition to authentication, confidentiality is optional as per IEC 62351 standard and is more challenging but in [156], they implemented the AES-GCM algorithm for both authentication and

encryption of message on both software and hardware levels and achieved promising results. These works focus on communication layer level to protect packets by different authentication and encryption algorithms mostly at IT level. These cyber security algorithms do not however account for the case of attack on the end device itself. To overcome this challenge, in literature researchers proposed artificial intelligence and machine learning based techniques which requires to gather and train a large amount of dataset in order to first classify different fault and attack categories and then take necessary actions [139, 155, 171, 172]. These methods require both storage and memory to process the dataset and then to perform according to pre-defined set of actions. The present works focus on either IT or OT levels, but holistic solution including both electrical and communication aspects is still a research gap. This work is an initial effort in this direction and propose an IT+OT based cybersecurity solution that can be implemented at the end device to secure it and take into consideration both communication and electrical aspects involved in these protocols and by using this knowledge, a novel mitigation method looking into the sequence and content of packets can be designed.

In this work, a novel cybersecurity solution is proposed and developed that takes into account the knowledge of unique identifiers and data items of the communication messages to mitigate cyberattacks. The unique identifiers represent the transmission sequence of packets and data items contain the electrical information. This method can be applied to time critical protocols such as GOOSE or SV of IEC-61850 standard. testbed is developed to simulate SV packets, modify them, evaluate their impact on the electrical network, and rectify the attack with a novel resolver. In case of any discrepancy, individual modules deal with the identified issues, e.g., the communication module will address a problem with the packet sequence, whereas

anomalous packet content can be rectified by the electrical module. The proposed solution is designed to be installed after ruling out system faults which is an independent module and out of scope of this work. If still the system is behaving abruptly, reason can be cyberattack only and it will be dealt by the sequence content resolver. The main research problem is to simulate cyberattacks (FDI attacks mainly masquerade and replay attacks) on SV protocol in real time digital simulator on a standard microgrid and later deploy mitigation technique to counter these attacks. Hence, the main contributions of this work are as follows:

1. Developed real time test bed for studying cyberattack (FDI) on SV protocol using RTDS, Snort and Wireshark.
2. Proposed novel IT+OT security scheme for securing SV protocol. Snort is used to inject FDI attacks and Wireshark is used to monitor the SV packets, an anti-Snort is proposed by the name of Sequence Content Resolver (SCR) which will nullify the impact of Snort and there will be cyberattack free communication between publisher and subscriber. SCR comprises of two modules i.e. COMM and ELEC, the former is the communication module which deals with the replay attacks (sequence of SV packets) and the latter is the electrical module which deals with the masquerade attacks (content of SV packets). Both modules together constitute SCR and mitigate the FDI attacks.
3. Demonstration of cyberattacks and proposed mitigation strategy on real time digital platform. The result of masquerade attack is presented in current and voltage waveforms to create a system fault alike situation on power system. The exploited SV packets effect the P&C IEDs which trip the breakers or generate islanding scenario in case of microgrid, this impact is evaluated, discussed and presented.

   Performance evaluation in terms of computational delays of the proposed IT+OT

scheme.

6.2. Cyberattacks on the SV Protocol and Impact on Electrical Network:

IEC 61850 is the de facto standard adopted worldwide for the automation of power systems. It defines different communication protocols for various devices (such as IEDs) to send and receive messages over Ethernet ensuring interoperability, remote monitoring, control and protection. The IEDs serve as the critical devices performing actions for smooth operation of a power plant depending on values of currents and voltages at various nodes. These values are measured and scaled down by current transformers (CTs) and voltage transformers (VTs) and then collected by MUs. These units communicate the values with protection IEDs via SV protocol. The protection IEDs decide to open or close the relevant circuit breakers based on this information. SV protocol sends the sampled values of voltage or current waveforms to IEDs at 80 or 256 samples/cycle for 50 or 60 Hz respectively. For each packet, the sample counter (smpCnt) is incremented from 0 to the upper limit (samples/cycle × frequency) and the transmission continues as long as the system is healthy.

In real world, the attacker's first objective is to access the substation's network. This is achieved by one or combination of the following vulnerabilities present in electrical substations connected with the control centre [164]:

1. Poorly configured gateways and firewalls
2. Weak passwords
3. Scanning of IP addresses, ports & services
4. Old OSs
5. USB flash drives
6. Shared internet
7. Weak network segmentation

Once the attacker gets access to network LAN by exploiting the aforementioned vulnerabilities, he can compromise one or multiple IEDs to achieve his malicious goals. As there is no security provided in SV protocol, it is a piece of cake for the attacker to compromise the MU and P&C IEDs and feed false data of sampled values to led the P&C IEDs into wrong tripping of multiple circuit breakers. This would be a very crucial and critical stage as the attacker becomes successful by corrupting the SV messages and should be addressed with sound and secure cybersecurity solutions.

Most of the cyberattacks are designed to malfunction IEDs because they collectively work as the brain of the power system. The attacks can be on IEDs' hardware, software and communication data it is receiving from other connected devices. In case of SV, the prime target of the attacker is to either manipulate the smpCnt or the data items in PhsMeas1 (decoding of seqData). The structure of a SV packet with its Wireshark capture are shown in Figure 6-2 and Figure 6-3. The parameters of Figure 6-3 which are of interest comes under Application Service Data Unit (ASDU) which are smpCnt and PhsMeas1. The former parameter represents the transmission sequence counter and keeps on resetting depending upon the system frequency while the latter contains instantaneous values of three phases and neutral values of currents and voltages. In smpCnt manipulation option, packets can be swapped or suppressed by considering smpCnt as unique identifier for each packet. In this attack, the packet will be genuine, but its time of transmission is exploited and are termed as replay attacks. In PhsMeas1 exploitation, the data values of the packets are played with, and the information being received in such case by the IED is not the actual sampled value. These attacks are called masquerade attacks. To make things more complicated, an attacker can do both also i.e., the time of delivery and contents of a particular SV packet can be exploited simultaneously making it difficult to realize the actual scenario.

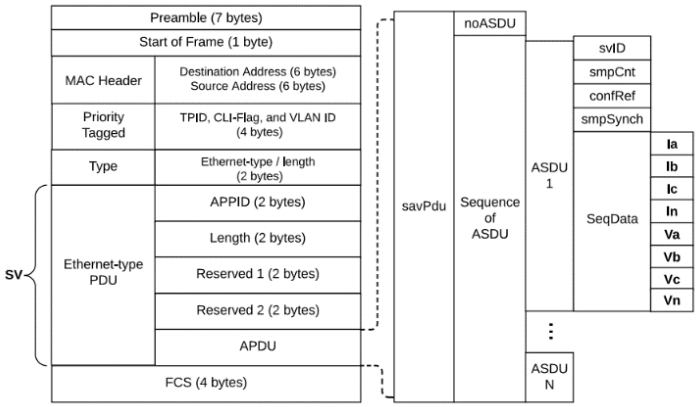


Figure 6-2. Structure of SV packet.

```
> Frame 442: 122 bytes on wire (976 bits),
> Ethernet II, Src: RTDSTech_0b:d9 (00:50:
v IEC61850 Sampled Values
    APPID: 0x4000
    Length: 108
    Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
  v savPdu
      noASDU: 1
    v seqASDU: 1 item
      v ASDU
            svID: EXE2MU0201
            smpCnt: 0
            confRef: 0
            smpSynch: local (1)
          > PhsMeas1
```

Figure 6-3. SV packet frame in Wireshark

The sampled measured values are basic input to the control IEDs for making protection decisions in times of fault and maintenance. In case of packet swapping, the IED can receive peak value in the beginning which is not intended, and the operators can act wrongly out of this information. If the packets are suppressed, the operators are basically in the dark and they would have no knowledge of the actual operating conditions of the equipment. In both these cases, the commands will be given manually to the protection IEDs by the operators. However, if the attacker is able to modify the contents of the SV packets, automatic tripping of circuit breakers can trigger provided the modified value is more than the pickup value of the relay which triggers the initial circuit breaker. The attack combining both exploitation of packet transmission and content will be more damaging on the electric grid. A representation of a substation

with various devices connected at different levels of buses is shown in Figure 6-4.

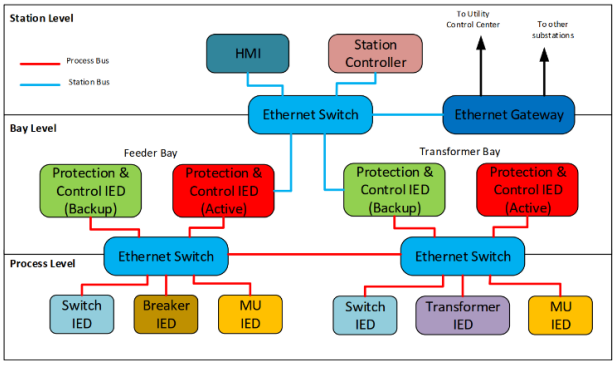


Figure 6-4. Devices at station, bay and process levels in a substation.

6.3. Proposed Mitigation Strategy:

In order to devise a strategy for FDI and masquerade attacks on SV packets, it has to be ruled out that the system is operating normally or under fault or maintenance [155]. If the conditions are neither normal nor faulty but the system is still behaving abruptly, then it must be a case of a cyberattack. To check electrically the system if it is normal or under some fault, one can implement a method by referring to the Historian (history of events) in a power plant. It basically records all the past events which happened in the system and is not considered in our work. Once, it is clear that the system is not working properly and the reason is neither physical nor electrical fault, one can look into the option of SV packet's manipulation, a possible option of attack which is tackled in this work. For the packet transmission order, smpCnt will play a vital role and the proposed solution will strictly checks the sequence of packets as received by the IEDs based on smpCnt. As smpCnt keeps on resetting, hence authentication of message is also mandatory as mentioned in IEC 62351-6 standard and can be performed by MAC algorithm to ensure data integrity and sender's legitimacy [156]. However, the MAC algorithms are symmetric cryptographic algorithms that require a secret key to be

shared between both publisher and subscriber. If the key is compromised the SV messages are exposed to different attacks. Hence, in addition of MAC based authentication (IT) additional security mechanism is required. The next objective in case of SV packets will be to ensure that a gradual increase or decrease in the sampled values is observed reflecting the behavior of a true sinusoidal wave for current or voltage consistent with that node in normal operating condition. These two actions will lay basis for a simple and fast rule based cybersecurity solution of SV packets at IT and OT levels.

Figure 6-5 presents the block diagram of the proposed method. After the fault is diagnosed properly and if still abrupt measurements are reported by MUs to P&C IEDs leading them to trigger unreal tripping commands, our solution can be deployed at the subscriber to inspect the SV packets being received. As shown in Figure 6-5, the packets with disrupted order will be dealt by the first communication module to block the replay attacks while together with the second electrical module, the device can defend against masquerade attacks by checking the data items. Once the fault is cleared, SV communication can be focused on between MUs and P&C IEDs, the counterfeit packets reaching the subscriber IEDs will pass first through the COMM module where based on the smpCnt, their sequence will be streamlined meaning if out of sequence packets are coming, they will be dropped and the output of COMM module is this representation. The next step for these packets is the ELEC module where based on PhsMeas1 content, the packets with ** will be matched with previous packets stored inside subscriber and with the publisher side also, only after that they will come out of ELEC module as authentic packets with ✓✓. The matching will be based on that the present packets are within tolerable range of current and voltage values present in PhsMeas1. Basically, the counterfeit packets will be dropped authenticating the SV

communication and integrity of P&C IED is ensured. This solution is implemented and tested in subsequent section and appropriate results are presented with proper discussion.

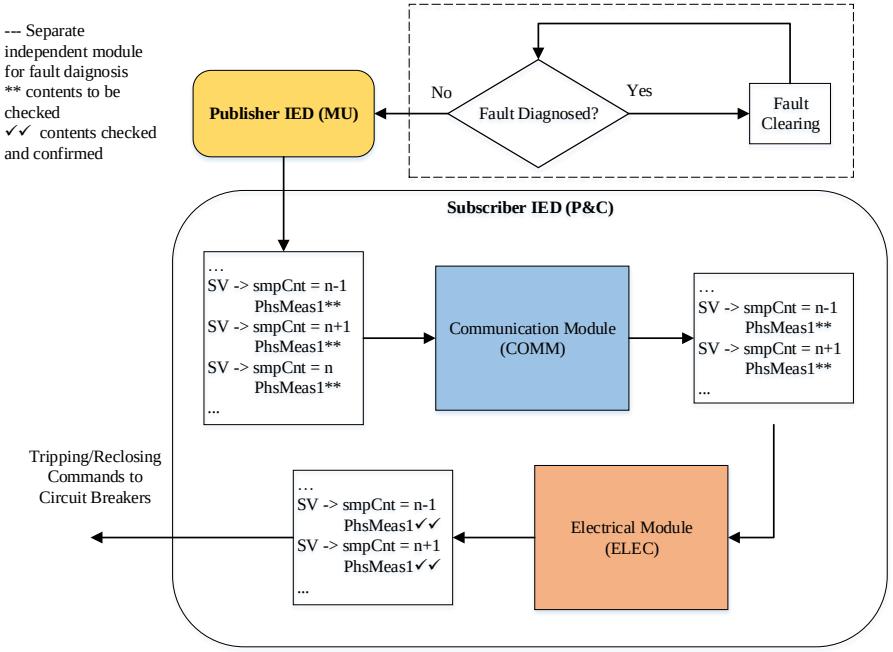


Figure 6-5. Block diagram of Sequence Content Resolver.

6.4. Simulation Results and Discussion:

In order to perform SV protocol simulation in real time in order to modify its packets for an attack and later implement its solution, a real time digital simulator (RTDS) [173] is considered as shown in Figure 6-6. The processer PB5 of the simulator is responsible to simulate the power system in consideration while its network interface card GTNETx2 simulate the automation protocols of IEC-61850 based power system such as SV. The publisher-subscriber represented by each module of GTNETx2 card is used for SV communication where publisher IED such as MU broadcast the sampled values while more than one P&C IEDs can subscribe to this data in multicast fashion. The rack and external switches allow this data to complete the loop over Ethernet while going

through Snort, an open source modified tool [160], used to modify the packets while simulating. The Wireshark and RSCAD in the workstation are used to monitor communication and electrical impact of this SV simulation and modification. RSCAD is the software counterpart of RTDS in which the power network under consideration is designed using its Draft window, compiled and then simulated in real time. Hence, the impact can be observed and evaluated of both attack and countermeasure in electrical domain inside Runtime window of RSCAD in real time.

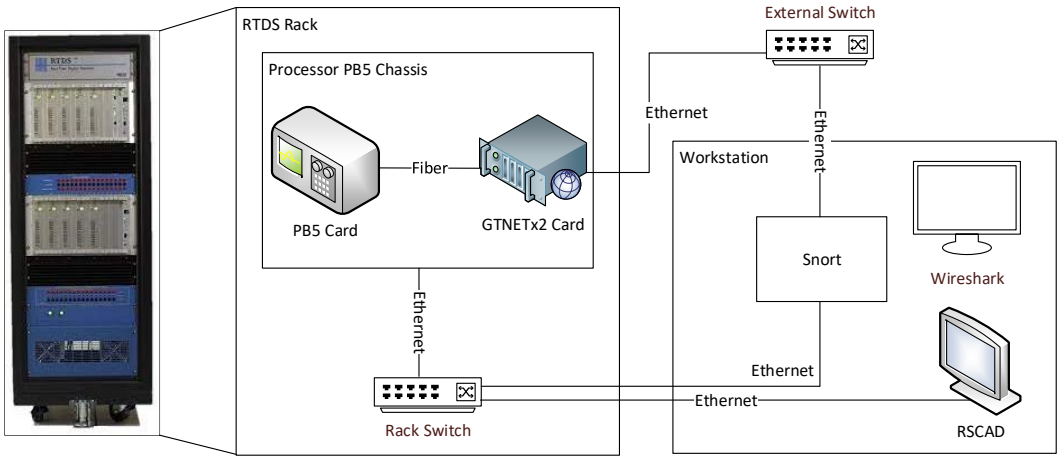
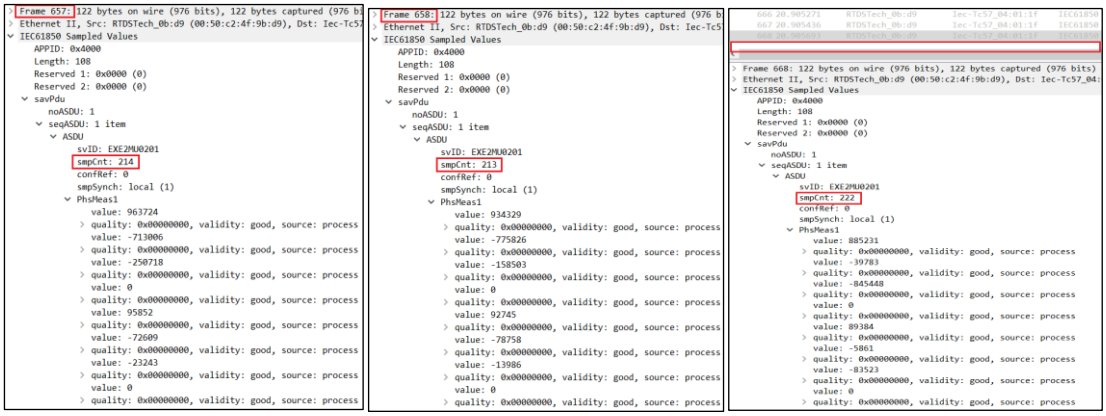


Figure 6-6. Testbed with RTDS, Wireshark and Snort.

6.4.1. Cyberattack on SV Packets

In order to demonstrate the methodology, the SV packets are simulated in real time between MU as publisher and protection and control (P&C) IED as subscriber via network interface card GTNETx2 of a real time digital simulator (RTDS). The SV packets are observed in Wireshark, depending on the sampling size (80 or 256 samples/cycle), the sampled values of a 3-phase voltage and current are transmitted with 80 samples/cycle representing the sinusoidal nature for both quantities. With sampling size of 256, 4 voltages and currents can be communicated instantly. It is interesting to note that the sampled values being transmitted are gradually changing and it is validated by following the correct sequence of SV packets in smpCnt. An attacker

can disrupt this communication by either disturbing the sequence of packets or modifying the sampled values to force P&C IEDs into issuing wrong commands to the circuit breakers of the interested zone. Conversely, an experienced attacker can directly attack the P&C IED to achieve the same objectives. Two such exploitations for attacking the order of packets are simulated as shown in Figure 6-7 (a), (b) and Figure 6-7 (c). The first case is packet swapping where the packets are captured and allowed after its successor; e.g. packet no. 213 will be transmitted after packet no. 214 where it should be other way around. In the second case, the packets are suppressed where at a pre-defined packet i.e., 222, the transmission will stop, or the succeeding packets will be dropped instead of reaching the subscriber IED.



(a) (b) (c)

Figure 6-7. Swapping of packets in Wireshark (a) packet with smpCnt = 214 should appear after the (b). (c) Dropping of packets in Wirashark (packets after smpCnt = 222 are dropped).

The attack can also be on the content of SV packets where the sampled values for currents or voltages are modified such that the intended circuit breakers are tripped through P&C IEDs. This modification is achieved by an open-source tool Snort in conjunction with RTDS. Snort basically captures the original packets and sends the modified counterparts to the targeted destination. Hence, in this case, the publisher MU

will send the original measurements of currents and voltages as sampled values, however, subscriber P&C IED will receive the modified data. Figure 6-8 shows the actual waveform (I_A, I_B, I_C) and its sampled counterpart (I_{Ain}, I_{Bin}, I_{Cin}) for 3-phase current after the attack where the corrupted sampled values are being received by the subscriber. The same false data injection is carried out with voltage, its waveform (N_1, N_2, N_3) and it sampled counterpart (V_{Ain}, V_{Bin}, V_{Cin}) after the attack are shown in Figure 6-9.

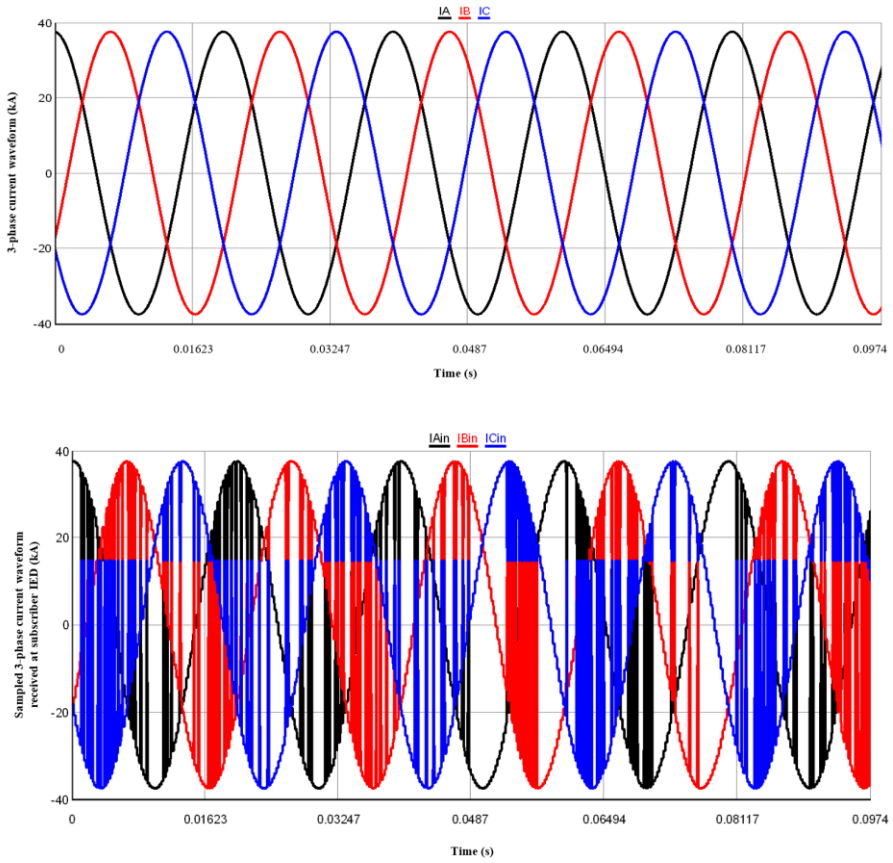


Figure 6-8. 3-phase current waveform at input of publisher (top) and received by subscriber (bottom) after attack.

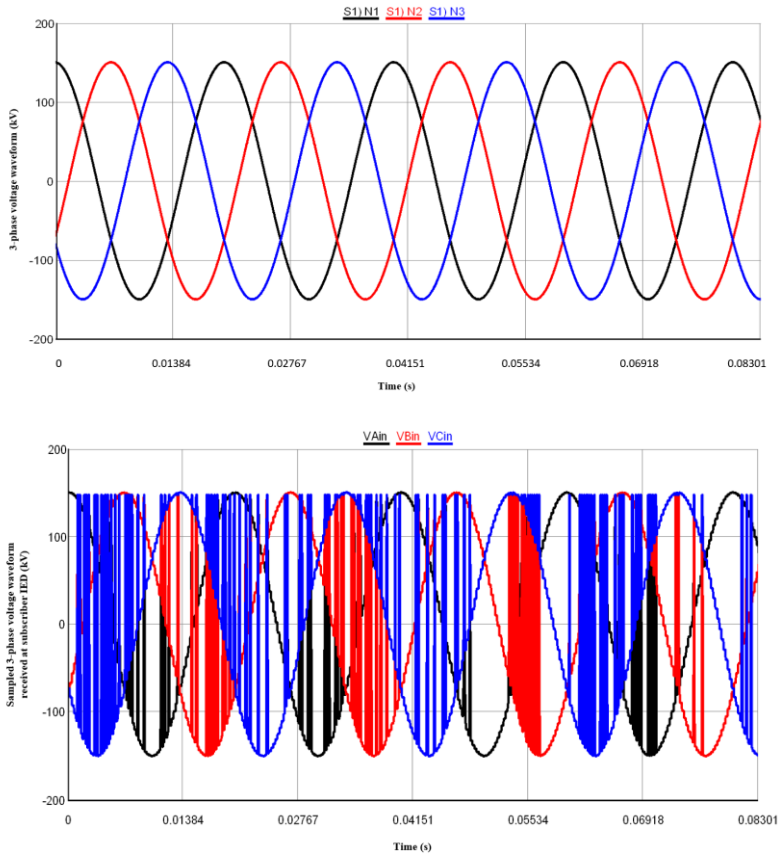


Figure 6-9. 3-phase voltage waveform at input of publisher (top) and received by subscriber (bottom) after attack.

This is the result of counterfeit SV packets with different smpCnt being received and having all the 8 data items for 3-phase current and voltage instant set to a higher fictitious value of 14766788 as shown in Figure 6-10. This type of FDI or masquerade attack corresponds to 3-phase to ground fault. Single-phase or double phase to ground fault can also be simulated by changing the corresponding phase values of currents and voltages to a higher number matching with the fault condition. Such simulations of modified communication packets constitute FDI attacks causing symmetric and asymmetric faults on electrical side. After evaluating the electrical impact, suitable mitigation techniques can be developed and employed to counter such attacks. Hence, it is established with our approach using real time simulation that SV packets can be manipulated by exploiting either their transmission sequence (smpCnt) or the content

of their data units (PhsMeas1) and can be a combination of both. Such attacks on SV packets give wrong information to P&C IEDs and they can be held hostage into issuing wrong commands such as tripping of multiple circuit breakers if the current values fed to them match to that of actual fault conditions.

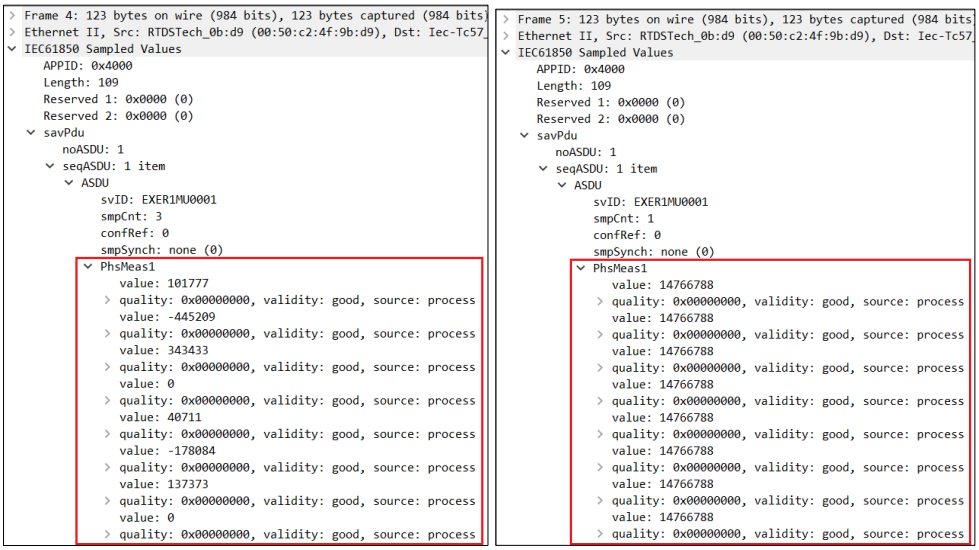


Figure 6-10. FDI attack (replay and masquearde) on data items of SV packets; left is the original packet while right is the packet after attack where all values are modified.

6.4.2. Evaluation of Impact on Electrical Side

After establishing the fact that SV packets can be delayed, dropped, modified and a combination of these, the impact of each on electrical side is evaluated. When the SV packets are delayed, this is a kind of wrong sequence of data being fed to subscriber IED which can be detrimental when combined with inflated or fault sampled values. The subscriber IED will not have any information when packets are dropped. In this window of opportunity, the subscriber IED can be accessed with alternative false data tending it to trigger unintended commands to the protection devices. The modification in the sampled values alone can also be translated as an abnormal event by the subscriber IED leading it to send false commands to the field devices. The impact can be manifold depending on the point and zone of attack. In case of an area breaker being

tripped by such an attack on SV packets, the effect will not be limited to that device but will trickle down towards downstream devices, equipment and loads. Without timely actions and security in place, the subsequent tripping can result in total blackout of the area.

Consider a three-area system connected to the grid in order to analyze the electrical effects of FDI attacks on SV protocol. The considered system is known as Banshee microgrid as shown in Figure 6-11. The point of interests in the system for an attacker will be the circuit breakers at multiple sites which can be directly controlled by GOOSE protocol. For indirect control, manipulated fault values can be fed via SV protocol to P&C IEDs in order to send tripping commands to the associated circuit breakers. The circuit breakers are installed at feeders, buses, transformers, tie-lines, loads, generators, and storage components of power systems. The tripping of component breakers will disconnect the downstream path such as loads, generators, transformers affecting consumers and creating electrical disturbances in the network. The tie-line breakers are kept normally opened and are closed only when neighboring areas can support each other in terms of power exchange. An attacker can misuse this condition too, but the worst-case scenario will be to trip the area or main feeder breaker from the grid. This will island the area putting pressure on the area's generation to meet the load demands. The system frequency will drop first, and the set points of area's generation will adjust themselves to continue feeding the loads. In case of inadequate generation, the interruptible loads will be shed first followed by priority and critical loads depending upon the gap between generation and demand.

The required sinusoidal waveform patterns will also be affected for generators and loads including motors creating disturbances in the electrical system. It affects the quality and integrity of consumers' supply and can damage the equipment if persisted

for long. Same behavior will be observed in both areas 1 and 3 as both have conventional generation i.e., diesel and natural gas fired respectively. Area 2 has PV and BESS and the storage system starts supplying power to the loads in case of islanding instead of saving it avoiding any load shedding. The BESS shifts its operating mode from PQ to VF when the area is disconnected from the grid. As PV is intermittent, the quality of supply to the loads will be affected if the area sustains on renewable energy for long without the backup of the main grid. The electrical impact of area islanding is summarized in Table 6-1. As the tripping commands can be wrongly issued by P&C IEDs mislead due to corrupted SV communication, it is critical to secure the SV communication for their proper functioning.

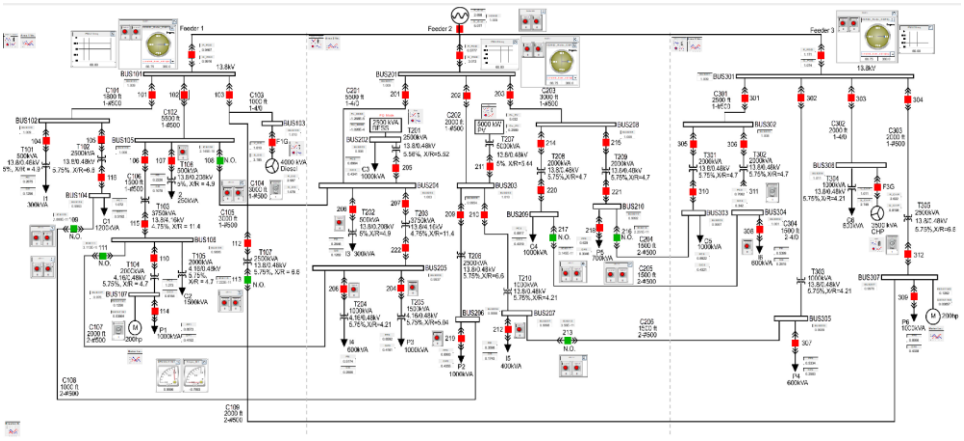


Figure 6-11. Runtime single line diagram of Banshee microgrid in RTDS.

Table 6-1. Comparison of main feeder breaker tripping, before and after, in the three areas of microgrid

Parameters	**Area 1**		**Area 2**		**Area 3**	
	Before islanding	*After islanding*	*Before islanding*	*After islanding*	*Before islanding*	*After islanding*
Frequency	60 Hz	59.55 Hz	60 Hz	59.5 Hz	60 Hz	59.56 Hz
Interruptible load shedding	None	I2	None	None	None	I6
Generation/Storage	P_DG= 2.997 MW Q_DG= 1.078 MVAR	P_DG= 3.518 MW Q_DG= 1.836 MVAR	BESS= PQ mode	BESS= VF mode	P_CHP= 2.622 MW Q_CHP= 0.8197 MVAR	P_CHP= 3.075 MW Q_CHP= 1.520 MVAR
Motor load	Sinusoidal	Non sinusoidal	NA	NA	Sinusoidal	Non sinusoidal

6.4.3. Implementation of Proposed Solution

In order to devise a cybersecurity solution to secure the manipulation of SV packets, the communication and electrical aspects of SV packets are perused, and the objective is to design a solution with minimum computing requirements considering the communication structure and electrical interpretation of SV packets. Hence the proposed solution is divided into communication and electrical modules to be deployed at device level on P&C IED. As described earlier, MAC algorithms is implemented to ensure data integrity and legitimacy of sender as smpCnt keeps on resetting after reaching its maximum value depending on the nominal frequency 50 Hz or 60 Hz as per the electrical case under consideration. Within this ramp of smpCnt (0 to MAX), the communication module will be responsible to verify the correct sequence of SV packets and its main input in this regard will be the parameter smpCnt of each received SV packet. The packets will be streamlined as a result and will be buffered waiting for their turn in case they are out of sequence. If the packets are dropped on the way, the subscriber IED will be intimidated to not issue any command until proper validation from the publisher IED is not acquired. For the content or sampled values available in

the SV packets, the electrical module will inspect them considering the pattern of sinusoidal current or voltage in the last cycle. The change of sampled values due to fault, switching or maintenance should have been ruled out by a previous module which is not the scope of this work. Hence, the SV packets are investigated at this stage only for a cyberattack on sequence (replay attack) or content (masquerade or FDI) of SV packets. After passing through both these modules, the authenticity of SV packets can be trusted completely by the subscriber IED and relevant commands can be issued to related devices based on this information.

The proposed solution originates from the basics of communication and electrical concepts and due to its simple nature, it guarantees a safe, secure and fast method to mitigate the attacks on SV packets from cyber domain. The implemented solution in subscriber IED is shown in Figure 6-12. The merging unit collects current and voltage measurements from the physical electrical nodes by CTs and PTs respectively and then send the sampled values to P&C IED over Ethernet by acting as a publisher. The SV packets are received by the subscriber and are checked for MAC authentication value by the communication (COMM) module. The packets are checked for sequence in case they passed the MAC authentication value check. In case the packets do not pass the MAC authentication value check, they are dropped with an alert. For the sequence, it refers to previous stored packet for comparison of smpCnt to check the transmission order of packets in order to divert replay attacks. If the sequence is disturbed, the problematic packets are blocked with an alert raised to intimate the sequence issue. The passed packets are then checked by the electrical (ELEC) module for the corresponding and gradual increase of node currents and voltages in sinusoidal pattern. Any spike in the sampled values will hold those packets to investigate the area of attack. The attack can be on the communication channel or on the publisher itself. The comparison of

previous packets received on the subscriber and the publisher will help to decide the source of attack and corresponding alarms will be raised. In this way, original packets will be allowed while counterfeit packets will be blocked based on the exploitation in sequence for replay attacks or in the data items for masquerade attacks from either communication channel or the publisher. The source of attack is also demarcated with appropriate alerts to further troubleshoot the area of attack or isolate it from the healthy zone at least.

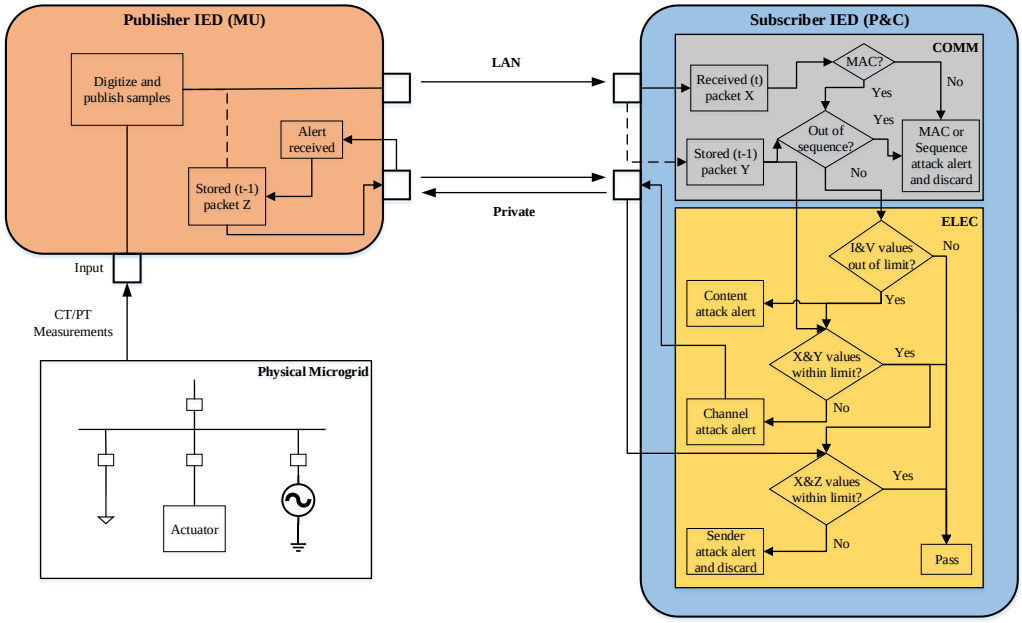


Figure 6-12. Functional diagram of Sequence Content Resolver

The impact of this countermeasure technique can be observed in the current and voltage waveforms of publisher and subscriber as shown in Figure 6-13 and Figure 6-14. The waveforms are clean and match the original date which was sent as compared to that of fake data injection which was observed earlier in Figure 6-8 and Figure 6-9. Conversely, on packet level capture from Wireshark, it is evident that original in-sequence packets (smpCnt = 3 & 4) are being received by P&C IED with the true data representation shown in Figure 6-15. This is different to the previous scenario in Figure 6-10 where fake data injection was carried out by the attacker resulting in out of order

packets (smpCnt = 3 & 1) with the latter containing the corrupted data items. Hence, the P&C IEDs will now be able to perform and issue genuine commands and any kind of exploitation on them via SV protocol will be mitigated by this solution. Moreover, the source and type of attack can also be traced down with the help of alarms being raised in different conditions. The proposed solution is light-weight due to its simple structure with basis on pure communication and electrical aspects of SV protocol and provides ease of implementation.

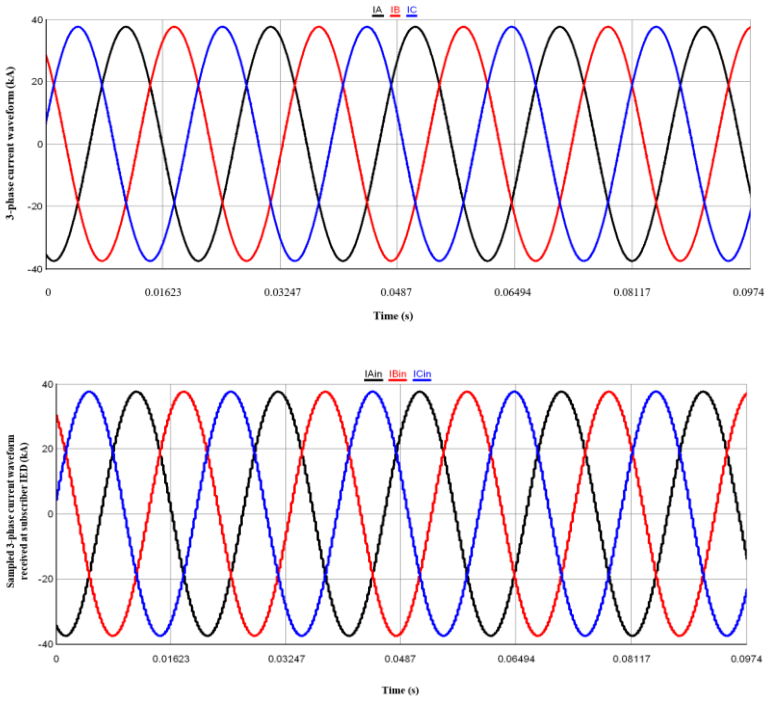


Figure 6-13. 3-phase current waveform at input of publisher (top) and received sampled waveform by subscriber (bottom) after mitigating the attack.

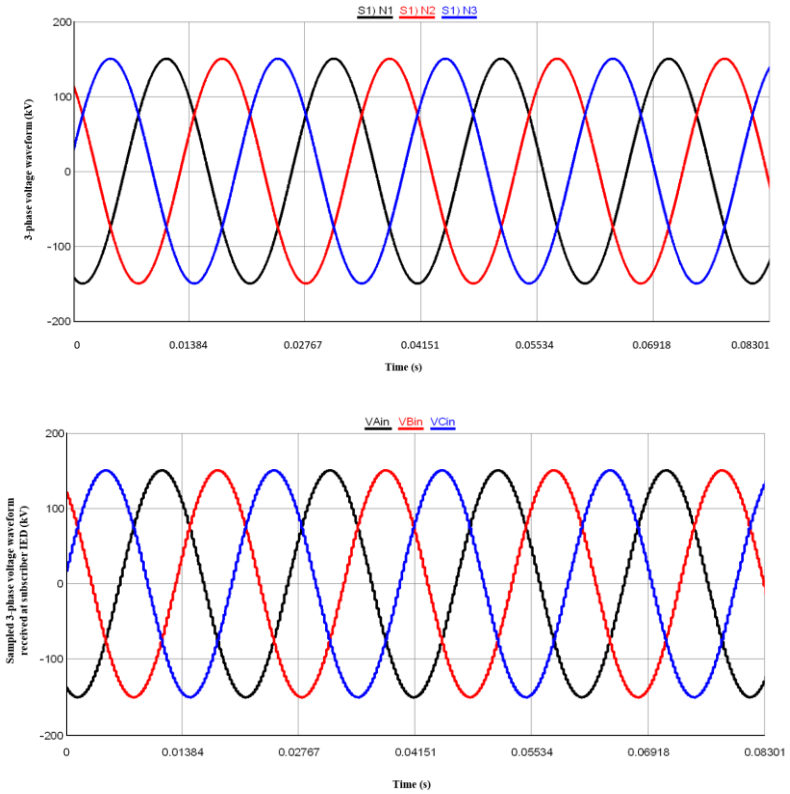


Figure 6-14. 3-phase voltage waveform at input of publisher (top) and received sampled waveform by subscriber (bottom) after mitigating the attack.

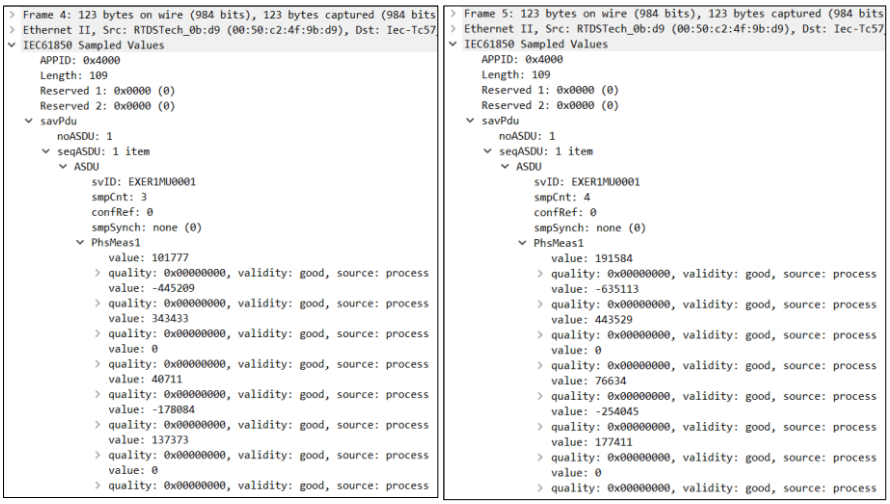


Figure 6-15. Normal SV packets in Wireshark after mitigating the attack.

In current literature, researchers have provided IT-based solutions, artificial intelligence based solutions but this is the first attempt as per our knowledge to provide an IT+OT based deterministic solution. The IT based solutions focuses on the communication security by authentication and encryption between the end devices.

Artificial intelligence is implemented on device level to secure it from attacks. The dataset is basically trained and classified to recognize attacks and faults from the normal scenario. This require storage and memory, hence IT+OT based is a simple and secure method for the cybersecurity at device level and is presented in this work. The qualitative features of the provided solutions in contemporary literature are summarized in Table 6-2.

Table 6-2. Cybersecurity solutions provided in literature on SV packets

	IT		**Artificial intelligence**	**IT+OT based deterministic**
	Authentication	Encryption		
M. Rodríguez et al. [156]	✓	✓	×	×
M. El Hariri et al. [139]	×	×	✓	×
T. S. Ustun et al. [155]	×	×	✓	×
This work	×	×	×	✓

6.4.4. Performance Evaluation

SV messages have very high messaging rates resulting in high throughputs and very low interarrival times. Figure 6-16 illustrates the interarrival times and communication network transmission delays for SV messages. The transmission delay is the time duration from publishing of SV packet at publisher to its arrival at subscriber, while inter-arrival is the time duration between arrivals of two consecutive SV packets at subscriber. The typical messaging rates of SV messages, as per the IEC 61850 standards, is 4000/4800 packets per second for 50/60 Hz system respectively. The interarrival times SV messages would be 0.24/0.21 ms. The performance will be sound if the time to probe the SV packet by proposed IT+OT scheme should be less than the interarrival times for SV packets to avoid congestion. Hence, the computational performance evaluation of the proposed IT+OT solution is presented in this section.

The proposed IT+OT solution has two main parts, i.e., implementation of MAC algorithms (IT) and sequence content resolver (OT). From [14] it has been observed that the computational delays for MAC algorithms is 0.007 ms. The computational time for executing the sequence content resolver is calculated. The difference in the time stamps of the simulation before and after the execution of sequence content resolver code gives the computational time elapsed. The simulation is performed for 100 sample value packets. The average computational delays for executing sequence content resolver is found to be 0.006 ms. Hence, the total computational delay is for the proposed IT+OT scheme is found to be 0.013 ms, which is well below the 0.21 ms limit. Table 6-3 shows the comparative computational performances of different security schemes in literature and proposed security scheme for SV messages. Hence, it can be safely concluded that the proposed security mechanism can be readily applied to time critical SV messages.

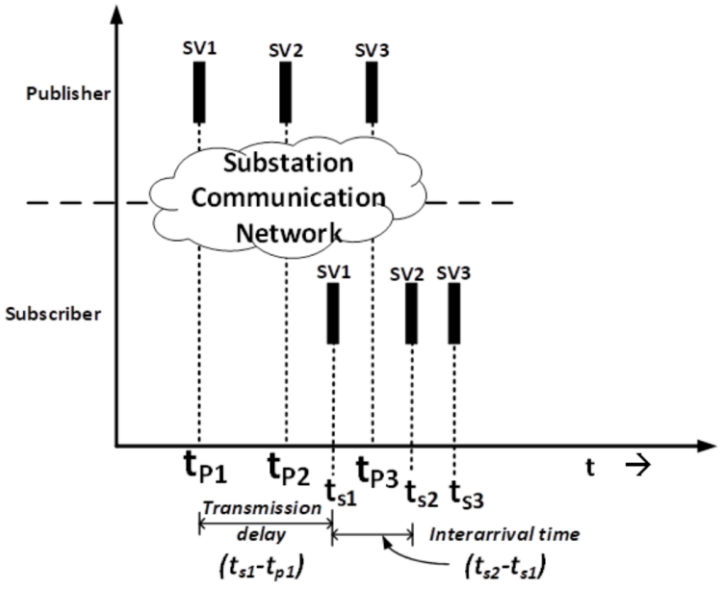


Figure 6-16. SV message exchange between a publisher and a subscriber.

Table 6-3. Computational delays of cybersecurity mechanism for SV packets

Method	Computational time in ms	Platform utilized	Lower than Inter-arrival time
M. Rodriguez et al. [156]	0.006	Zynq 7020 FPGA	✓
M. El Hariri et al. [139]	0.29	ODROID C2 microcontroller	✓
T. S. Ustun et al. [155]	0.049	Intel Core i7 @ 2.80 GHz 32 GB RAM	✓
This work	0.013	Intel Core i7 @ 1.80 GHz 16 GB RAM	✓

6.5. Summary:

In this work, SV protocol is tackled from cyberattack or false data injection perspective. The packets are simulated in real time, modified and their impact on electrical network is evaluated. The exploitation of SV communication is carried out from attacker's perspective to corrupt the packets by replay and/or masquerade attacks. This is to take indirect route via P&C IEDs in order to feed wrong data leading the IEDs to issue false tripping commands. Both the consumers and equipment will be affected in absence of any proper countermeasure. A novel light-weight sequence-content resolver is designed and implemented to mitigate the attacks on SV protocol. It encompasses both the communication and electrical aspects of the packets and depending upon that, a holistic IT and OT based cybersecurity solution with required and promising results is achieved to counter the type of attacks carried out on SV communication and MUs in the form of replay and masquerade attacks. The computational performance evaluations show that the proposed IT+OT scheme can be safely applied to the SV messages. Future studies will be to increase the performance of the proposed method and extend it to the other time critical protocol namely GOOSE in the same fashion. Moreover, the

principles of artificial intelligence will be explored for relaxed and legacy protocols used in automated power system.

CHAPTER 7: Conclusion and Future work:

Conclusion

In this work, contribution has been done to the body of knowledge by solving pertinent problems in conventional grid, renewable energy based system and IEC-61850 based smart grid.

- In conventional grid, the classical problem of combined economic and emission dispatch is resolved by using two pioneer swarm intelligence methods i.e. particle swarm optimization and genetic algorithm. Moreover, their performance is compared and results are presented. The combined dispatch of plant generators with respect to fuel and gas emissions was carried out using PSO and GA in MATLAB. The results demonstrate that PSO outperforms GA for the combined dispatch in terms of achieving lower fuel cost, lower emission, fast convergence, and lesser simulation time. This was validated for both IEEE 30 bus system and for an independent power plant with simulation, 3D plots, and thorough discussion. The work has successfully implemented PSO and GA algorithms for CEED of the same systems. The simulation results are compared and tabulated for different load demands. 3D plots were discussed to highlight the convergence characteristics of PSO and GA with respect to fuel cost and gas emissions.
- In renewable energy based system, the optimal sizing of photovoltaic-wind turbine-battery energy storage system is tackled by inventing a superior novel technique called iterative-filter-selection approach over iterative-pareto-fuzzy and particle swarm optimization techniques. A new optimization method has been introduced in this work named iterative filter selection (IFS) approach for

optimization problems and applied on PV-WT-Battery system. The method is compared with iterative-pareto-fuzzy and particle swarm optimization techniques and found superior in terms of system cost and dump load size satisfying higher load demand. Its computational time is also small because of its simple algorithmic structure. Some parameters like reliability tolerance and dump load size tolerance have been refined for better and fast results. Maximum number of batteries is considered only, to minimize dump load size due to which total solutions also decreased by five times compared to previous work using iterative-pareto-fuzzy technique. The best solution given by IFS approach has lowest cost, optimized reliability and no dump load for the duration of analysis.

- In smart grid, the two time stringent protocols i.e. GOOSE and SV as defined in the universal automation standard IEC-61850 are exploited by introducing false data injection (FDI) attacks in real time digital simulator (RTDS). The effects of FDI attacks are studied and rule based cybersecurity solutions are devised and contributed which deals with securing the protocols at communication level as well as consider the electrical aspects to provide holistic and hybrid novel methodologies for both protocols.
- For GOOSE protocol, a methodology to validate cyberattacks and evaluate their impact on power systems is established with the help of a testbed focusing on GOOSE, the most critical protocol utilized for implementing protection. The protocol has been implemented, and modified GOOSE messages have been sent to a simulated electrical system in order to observe its impact. This allowed us to investigate the electrical effects and discuss broad categories of countermeasures. A holistic cybersecurity solution named as Sequence Content resolver is also proposed and implemented using the same test bed.

- SV protocol is tackled from cyberattack or false data injection perspective. The packets are simulated in real time, modified and their impact on electrical network is evaluated. The exploitation of SV communication is carried out from attacker's perspective to corrupt the packets by replay and/or masquerade attacks. This is to take indirect route via P&C IEDs in order to feed wrong data leading the IEDs to issue false tripping commands. Both the consumers and equipment will be affected in absence of any proper countermeasure. A novel light-weight sequence-content resolver is designed and implemented to mitigate the attacks on SV protocol. It encompasses both the communication and electrical aspects of the packets and depending upon that, a holistic IT and OT based cybersecurity solution with required and promising results is achieved to counter the type of attacks carried out on SV communication and MUs in the form of replay and masquerade attacks. The computational performance evaluations show that the proposed IT+OT scheme can be safely applied to the SV messages.

Future Work

The future work will deal with advancing the work in smart grid and IEC-61850 standard by exploiting other protocols such as MMS and SNTP and providing and comparing with other artificial intelligence solutions such as supervised learning and ensemble methods. The work will be carried out in RTDS and moreover, the routable versions of GOOSE and SV i.e. R-GOOSE and R-SV will also be tackled in future studies as their access go beyond substations to entire power system considering the fact that IEC-61850 standard is expanding towards the whole power system automation. Overall, the cyberattacks in IEC-61850 standard's protocols in RTDS using artificial intelligence (AI), machine learning and deep learning will be considered. The standard

cases of conventional grid with renewables integration will be studied for dealing with the problems or faults or cyberattacks in the power system and later deploy AI based models to mitigate the issues at hand. For GOOSE, future work will make the solution more robust and explore other IEC-61850 based communication protocols for vulnerabilities such as SV and MMS. Further, advanced mitigation methods will be developed to secure devices and communication inside automated power systems while fulfilling the strict performance requirements for these environments. For SV, future studies will be to increase the performance of the proposed method and extend it to the other protocols in the same fashion. Moreover, the principles of artificial intelligence will be explored for relaxed and legacy protocols used in automated power system.

References:

[1] E. Gonçalves, A. R. Balbo, D. N. da Silva, L. Nepomuceno, E. C. Baptista, and E. M. Soler, "Deterministic approach for solving multi-objective non-smooth Environmental and Economic dispatch problem," *International Journal of Electrical Power & Energy Systems,* vol. 104, pp. 880-897, 2019.

[2] F. P. Mahdi, P. Vasant, V. Kallimani, J. Watada, P. Y. S. Fai, and M. Abdullah-Al-Wadud, "A holistic review on optimization strategies for combined economic emission dispatch problem," *Renewable and Sustainable Energy Reviews,* vol. 81, pp. 3006-3020, 2018.

[3] S. K. Mishra and S. K. Mishra, "A comparative study of solution of economic load dispatch problem in power systems in the environmental perspective," *Procedia computer science,* vol. 48, pp. 96-100, 2015.

[4] D. P. Kothari, "Power system optimization," in *2012 2nd National Conference on Computational Intelligence and Signal Processing (CISP)*, 2012, pp. 18-21.

[5] M. R. AlRashidi and M. E. El-Hawary, "Emission-economic dispatch using a novel constraint handling particle swarm optimization strategy," in *2006 Canadian Conference on Electrical and Computer Engineering*, 2006, pp. 664-669.

[6] T. C. Bora, V. C. Mariani, and L. dos Santos Coelho, "Multi-objective optimization of the environmental-economic dispatch with reinforcement learning based on non-dominated sorting genetic algorithm," *Applied Thermal Engineering,* vol. 146, pp. 688-700, 2019.

[7] P. Ghamisi and J. A. Benediktsson, "Feature selection based on hybridization of genetic algorithm and particle swarm optimization," *IEEE Geoscience and remote sensing letters,* vol. 12, pp. 309-313, 2015.

[8] H. Jiang, Y. Zhang, and H. Xu, "Optimal allocation of cooperative jamming resource based on hybrid quantum-behaved particle swarm optimisation and genetic algorithm," *IET Radar, Sonar & Navigation,* vol. 11, pp. 185-192, 2016.

[9] J. Wang, F. Zhang, F. Liu, and J. Ma, "Hybrid forecasting model-based data mining and genetic algorithm-adaptive particle swarm optimisation: a case study of wind speed time series," *IET Renewable Power Generation,* vol. 10, pp. 287-298, 2016.

[10] S. N. Ohatkar and D. S. Bormane, "Hybrid channel allocation in cellular network based on genetic algorithm and particle swarm optimisation methods," *Iet Communications,* vol. 10, pp. 1571-1578, 2016.

[11] R. Villarroel, D. García, M. Dávila, and E. Caicedo, "Particle swarm optimization vs genetic algorithm, application and comparison to determine the moisture diffusion coefficients of pressboard transformer insulation," *IEEE Transactions on Dielectrics and Electrical Insulation,* vol. 22, pp. 3574-3581, 2015.

[12] H. Liang, Y. Liu, F. Li, and Y. Shen, "A multiobjective hybrid bat algorithm for combined economic/emission dispatch," *International Journal of Electrical Power & Energy Systems,* vol. 101, pp. 103-115, 2018.

[13] B. Lokeshgupta and S. Sivasubramani, "Multi-objective dynamic economic and emission dispatch with demand side management," *International Journal of Electrical Power & Energy Systems,* vol. 97, pp. 334-343, 2018.

[14] U. Güvenç, Y. Sönmez, S. Duman, and N. Yörükeren, "Combined economic and emission dispatch solution using gravitational search algorithm," *Scientia Iranica,* vol. 19, pp. 1754-1762, 2012.

[15] L. Jebaraj, C. Venkatesan, I. Soubache, and C. C. A. Rajan, "Application of

differential evolution algorithm in static and dynamic economic or emission dispatch problem: a review," *Renewable and Sustainable Energy Reviews,* vol. 77, pp. 1206-1220, 2017.

[16] Q. Niu, H. Zhang, X. Wang, K. Li, and G. W. Irwin, "A hybrid harmony search with arithmetic crossover operation for economic dispatch," *International journal of electrical power & energy systems,* vol. 62, pp. 237-257, 2014.

[17] M. Nazari-Heris, B. Mohammadi-Ivatloo, and G. Gharehpetian, "A comprehensive review of heuristic optimization algorithms for optimal combined heat and power dispatch from economic and environmental perspectives," *Renewable and Sustainable Energy Reviews,* vol. 81, pp. 2128-2143, 2018.

[18] G. Müller-Fürstenberger and M. Wagner, "Exploring the environmental Kuznets hypothesis: Theoretical and econometric problems," *Ecological Economics,* vol. 62, pp. 648-660, 2007.

[19] P. J. Straatman and W. G. van Sark, "A New Hybrid Ocean Thermal Energy Conversion-Offshore Solar Pond (OTEC-OSP) Design: A Cost Optimization Approach," in *Renewable Energy,* ed: Routledge, 2018, pp. 501-513.

[20] A. Akella, R. Saini, and M. P. Sharma, "Social, economical and environmental impacts of renewable energy systems," *Renewable Energy,* vol. 34, pp. 390-396, 2009.

[21] O. H. Mohammed, Y. Amirat, G. Feld, and M. Benbouzid, "Hybrid Generation Systems Planning Expansion Forecast State of the Art Review: Optimal Design vs Technical and Economical Constraints," *Journal of Electrical Systems,* vol. 12, 2016.

[22] G. Privitera, A. R. Day, G. Dhesi, and D. Long, "Optimising the installation

costs of renewable energy technologies in buildings: a linear programming approach," *Energy and Buildings*, vol. 43, pp. 838-843, 2011.

[23] S. Diaf, D. Diaf, M. Belhamel, M. Haddadi, and A. Louche, "A methodology for optimal sizing of autonomous hybrid PV/wind system," *Energy policy*, vol. 35, pp. 5708-5718, 2007.

[24] S. Diaf, M. Belhamel, M. Haddadi, and A. Louche, "Technical and economic assessment of hybrid photovoltaic/wind system with battery storage in Corsica island," *Energy policy*, vol. 36, pp. 743-754, 2008.

[25] S. Diaf, G. Notton, M. Belhamel, M. Haddadi, and A. Louche, "Design and techno-economical optimization for hybrid PV/wind system under various meteorological conditions," *Applied Energy*, vol. 85, pp. 968-987, 2008.

[26] W. Shen, "Optimally sizing of solar array and battery in a standalone photovoltaic system in Malaysia," *Renewable energy*, vol. 34, pp. 348-352, 2009.

[27] A. K. Bansal, R. Gupta, and R. Kumar, "Optimization of hybrid PV/wind energy system using Meta Particle Swarm Optimization (MPSO)," in *India International Conference on Power Electronics 2010 (IICPE2010)*, 2011, pp. 1-7.

[28] K. Kusakana and H. Vermaak, "Hybrid Photovoltaic-Wind system as power solution for network operators in the DR Congo," in *2011 international conference on Clean electrical power (ICCEP)*, 2011, pp. 703-708.

[29] K. Sopian, A. Zaharim, Y. Ali, Z. M. Nopiah, J. A. Razak, and N. S. Muhammad, "Optimal operational strategy for hybrid renewable energy system using genetic algorithms," *WSEAS Transactions on Mathematics*, vol. 7, pp. 130-140, 2008.

[30] R. Mukhtaruddin, H. Rahman, M. Hassan, and J. Jamian, "Optimal hybrid renewable energy design in autonomous system using Iterative-Pareto-Fuzzy technique," *International Journal of Electrical Power & Energy Systems,* vol. 64, pp. 242-249, 2015.

[31] M. S. Ismail, M. Moghavvemi, and T. Mahlia, "Genetic algorithm based optimization on modeling and design of hybrid renewable energy systems," *Energy Conversion and Management,* vol. 85, pp. 120-130, 2014.

[32] A. Fetanat and E. Khorasaninejad, "Size optimization for hybrid photovoltaic–wind energy system using ant colony optimization for continuous domains based integer programming," *Applied Soft Computing,* vol. 31, pp. 196-209, 2015.

[33] P. Suhane, S. Rangnekar, and A. Mittal, "Optimal sizing of hybrid energy system using ant colony optimization," *International Journal of Renewable Energy Research,* vol. 4, pp. 683-688, 2014.

[34] A. Maleki and A. Askarzadeh, "Artificial bee swarm optimization for optimum sizing of a stand-alone PV/WT/FC hybrid system considering LPSP concept," *Solar Energy,* vol. 107, pp. 227-235, 2014.

[35] T. Khatib, A. Mohamed, and K. Sopian, "Optimization of a PV/wind micro-grid for rural housing electrification using a hybrid iterative/genetic algorithm: Case study of Kuala Terengganu, Malaysia," *Energy and Buildings,* vol. 47, pp. 321-331, 2012.

[36] R. Bayindir, I. Colak, G. Fulli, and K. Demirtas, "Smart grid technologies and applications," *Renewable and Sustainable Energy Reviews,* vol. 66, pp. 499-516, 2016.

[37] G. N. Sorebo and M. C. Echols, *Smart grid security: an end-to-end view of*

security in the new electrical grid: CRC Press, 2016.

[38] I. Ali and S. S. Hussain, "Control and management of distribution system with integrated DERs via IEC 61850 based communication," *Engineering science and technology, an international journal,* vol. 20, pp. 956-964, 2017.

[39] J. R. Agüero, E. Takayesu, D. Novosel, and R. Masiello, "Grid modernization: challenges and opportunities," *The Electricity Journal,* vol. 30, pp. 1-6, 2017.

[40] H. Wang, B. Zhou, and X. Zhang, "Research on the Remote Maintenance System Architecture for the Rapid Development of Smart Substation in China," *IEEE Transactions on Power Delivery,* vol. 33, pp. 1845-1852, 2018.

[41] M. Wei and W. Wang, "Data-centric threats and their impacts to real-time communications in smart grid," *Computer Networks,* vol. 104, pp. 174-188, 2016.

[42] A. S. Bretas, N. G. Bretas, B. Carvalho, E. Baeyens, and P. P. Khargonekar, "Smart grids cyber-physical security as a malicious data attack: An innovation approach," *Electric Power Systems Research,* vol. 149, pp. 210-219, 2017.

[43] Y. Zhang, W. Chen, and W. Gao, "A survey on the development status and challenges of smart grids in main driver countries," *Renewable and Sustainable Energy Reviews,* vol. 79, pp. 137-147, 2017.

[44] R. Leszczyna, "Cybersecurity and privacy in standards for smart grids–A comprehensive survey," *Computer Standards & Interfaces,* vol. 56, pp. 62-73, 2018.

[45] R. Leszczyna, "A Review of Standards with Cybersecurity Requirements for Smart Grid," *Computers & Security,* pp. 262-276, 2018.

[46] I. Colak, S. Sagiroglu, G. Fulli, M. Yesilbudak, and C.-F. Covrig, "A survey on the critical issues in smart grid technologies," *Renewable and Sustainable*

Energy Reviews, vol. 54, pp. 396-405, 2016.

[47] N. Moreira, E. Molina, J. Lázaro, E. Jacob, and A. Astarloa, "Cyber-security in substation automation systems," *Renewable and Sustainable Energy Reviews,* vol. 54, pp. 1552-1562, 2016.

[48] S. K. Venkatachary, J. Prasad, and R. Samikannu, "Cybersecurity and cyber terrorism-in energy sector–a review," *Journal of Cyber Security Technology,* vol. 2, pp. 111-130, 2018.

[49] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, "Cyber-security in smart grid: Survey and challenges," *Computers & Electrical Engineering,* vol. 67, pp. 469-482, 2018.

[50] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer Networks,* vol. 169, p. 107094, 2020.

[51] S. Nazir, S. Patel, and D. Patel, "Assessing and augmenting SCADA cyber security: A survey of techniques," *Computers & Security,* vol. 70, pp. 436-454, 2017.

[52] Z. Yang, C.-W. Ten, and A. Ginter, "Extended enumeration of hypothesized substations outages incorporating overload implication," *IEEE Transactions on Smart Grid,* vol. 9, pp. 6929-6938, 2018.

[53] W. Tong, J. Gao, Z. Li, and X. Jing, "A Protection Method Based on Message Identification and Flow Monitoring for Managing the Congestion Arising from Network Attacks on Smart Substation," *IEEE Communications Letters,* 2018.

[54] J. Hong and C.-C. Liu, "Intelligent electronic devices with collaborative intrusion detection systems," *IEEE Transactions on Smart Grid,* vol. 10, pp. 271-281, 2019.

[55] A. Jindal, A. K. Marnerides, A. Gouglidis, A. Mauthe, and D. Hutchison,

"Communication standards for distributed renewable energy sources integration in future electricity distribution networks," in *ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2019, pp. 8390-8393.

[56] Y. Kabalci, "A survey on smart metering and smart grid communication," *Renewable and Sustainable Energy Reviews,* vol. 57, pp. 302-318, 2016.

[57] R. H. Khan and J. Y. Khan, "A comprehensive review of the application characteristics and traffic requirements of a smart grid communications network," *Computer Networks,* vol. 57, pp. 825-845, 2013.

[58] S. Marzal, R. Salas, R. González-Medina, G. Garcerá, and E. Figueres, "Current challenges and future trends in the field of communication architectures for microgrids," *Renewable and Sustainable Energy Reviews,* vol. 82, pp. 3610-3622, 2018.

[59] L. Shi, Q. Dai, and Y. Ni, "Cyber–physical interactions in power systems: A review of models, methods, and applications," *Electric Power Systems Research,* vol. 163, pp. 396-412, 2018.

[60] "Smart Grid projects in Europe: lessons learned and current developments," JRC Reference Reports 2011.

[61] "Adoption of Smart Grid Technologies: Results of a Survey of U.S. Electric Utilities," 2016.

[62] "Smart Grid Drivers and Technologies by Country, Economy, and Continent," ISGAN Framework of Assessment Report2014.

[63] R. Kowalik, D. D. Rasolomampionona, and M. Januszewski, "Laboratory testing of process bus equipment and protection functions in accordance with IEC 61850 standard. Part I: Electrical arrangement and basic protection

functions tests," *International Journal of Electrical Power & Energy Systems,* vol. 90, pp. 54-63, 2017.

[64] R. Kowalik, D. D. Rasolomampionona, and M. Januszewski, "Laboratory testing of process bus equipment and protection functions in accordance with IEC 61850 standard: Part II: Tests of protection functions in a LAN-based environment," *International Journal of Electrical Power & Energy Systems,* vol. 94, pp. 405-414, 2018.

[65] H. Hajian-Hoseinabadi, "Reliability and component importance analysis of substation automation systems," *International Journal of Electrical Power & Energy Systems,* vol. 49, pp. 455-463, 2013.

[66] J. Hong, "Cyber security of substation automation systems, PhD Thesis," 2014.

[67] J. Jarmakiewicz, K. Maślanka, and K. Parobczak, "Evaluation of the cyber security provision system for critical infrastructure," *Journal of Telecommunications and Information Technology,* pp. 22-29, 2015.

[68] C. Wueest, "Targeted attacks against the energy sector," *Symantec Security Response, Mountain View, CA,* 2014.

[69] A. Dreher and G. Fernandez, "Cyber security in electrical substations," *Hirschmann, Belden, USA,* 2015.

[70] S. Poudel, Z. Ni, and N. Malla, "Real-time cyber physical system testbed for power system security and control," *International Journal of Electrical Power & Energy Systems,* vol. 90, pp. 124-133, 2017.

[71] M. Annor-Asante and B. Pranggono, "Development of smart grid testbed with low-cost hardware and software for cybersecurity research and education," *Wireless Personal Communications,* pp. 1-21, 2018.

[72] "Kaspersky Lab, Industrial CyberSecurity Conference: Unite and Act (2016),"

Available at: <https://ics.kaspersky.com/conference-2016/> [Accessed on: 10/2020].

[73] D. Kushner, "The real story of stuxnet," *ieee Spectrum*, vol. 3, pp. 48-53, 2013.

[74] C. Bronk and E. Tikk-Ringas, "The cyber attack on Saudi Aramco," *Survival*, vol. 55, pp. 81-96, 2013.

[75] D. D. Cheong, "Cyberattacks in the Gulf: lessons for active defence," 2012.

[76] D. U. Case, "Analysis of the cyber attack on the Ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, 2016.

[77] M. Amanowicz and J. Jarmakiewicz, "Cyber Security Provision for Industrial Control Systems," in *Polish Control Conference*, 2017, pp. 611-620.

[78] C. Moya, J. Hong, and J. Wang, "Application of Correlation Indices on Intrusion Detection Systems: Protecting the Power Grid Against Coordinated Attacks," *arXiv preprint arXiv:1806.03544*, 2018.

[79] R. Fu, X. Huang, Y. Xue, Y. Wu, Y. Tang, and D. Yue, "Security assessment for cyber physical distribution power system under intrusion attacks," *IEEE Access*, 2018.

[80] A. Jindal, A. K. Marnerides, A. Scott, and D. Hutchison, "Identifying Security Challenges in Renewable Energy Systems: A Wind Turbine Case Study," in *Proceedings of the Tenth ACM International Conference on Future Energy Systems*, 2019, pp. 370-372.

[81] P. Systems and S. Automation, "Cyber security for substation automation systems by ABB," *ABB Switzerland Ltd.*, 2010.

[82] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *International Journal of Electrical Power & Energy Systems*, vol. 99, pp. 45-56, 2018.

[83] "Lanner, 5 Common Vulnerabilities in Industrial Control Systems (2017)," *Available at: <https://www.lanner-america.com/blog/5-common-vulnerabilities-industrial-control-systems/> [Accessed on: 03/2020]*.

[84] Y. Xiang, L. Wang, and Y. Zhang, "Adequacy evaluation of electric power grids considering substation cyber vulnerabilities," *International Journal of Electrical Power & Energy Systems,* vol. 96, pp. 368-379, 2018.

[85] S. S. Hussain, M. A. Aftab, and I. Ali, "A novel PRP based deterministic, redundant and resilient IEC 61850 substation communication architecture," *Perspectives in Science,* vol. 8, pp. 747-750, 2016.

[86] I. Ali, M. S. Thomas, S. Gupta, and S. S. Hussain, "IEC 61850 substation communication network architecture for efficient energy system automation," *Energy Technology & Policy,* vol. 2, pp. 82-91, 2015.

[87] I. P. H. W. Group, "Application consideration of IEC 61850/UCA2 for substation Ethernet local area network communication for protection and control," Tech. Rep, May2005.

[88] D. S. Pidikiti, R. Kalluri, R. S. Kumar, and B. Bindhumadhava, "SCADA communication protocols: vulnerabilities, attacks and possible mitigations," *CSI transactions on ICT,* vol. 1, pp. 135-141, 2013.

[89] Q. S. Qassim, N. Jamil, M. Daud, N. Ja'affar, S. Yussof, R. Ismail, *et al.*, "Simulating command injection attacks on IEC 60870-5-104 protocol in SCADA system," *International Journal of Engineering & Technology,* vol. 7, pp. 153-159, 2018.

[90] M. Kerkers, "Assessing the security of IEC 60870-5-104 implementations using automata learning," University of Twente, 2017.

[91] M. J. Gonzalez-Redondo, A. Moreno-Munoz, V. Pallares-Lopez, and R. J. Real-

Calvo, "Influence of data-related factors on the use of IEC 61850 for power utility automation," *Electric Power Systems Research,* vol. 133, pp. 269-280, 2016.

[92] E. Molina, E. Jacob, J. Matias, N. Moreira, and A. Astarloa, "Using software defined networking to manage and control IEC 61850-based systems," *Computers & Electrical Engineering*, vol. 43, pp. 142-154, 2015.

[93] F. Cleveland, "IEC TC57 WG15: IEC 62351 security standards for the power system information infrastructure," *White Paper,* 2012.

[94] NCCIC and ICS-CERT, "NCCIC/ICS-CERT Year in Review (2015)," *Available at: <https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf> [Accessed on: 03/2020]*.

[95] E. Cosman. (2017). *Do we need to debate the relative drivers behind ICS Cybersecurity?* Available: https://www.arcweb.com/blog/do-we-need-debate-relative-drivers-behind-ics-cybersecurity

[96] M. Hajizadeh, T. V. Phan, and T. Bauschert, "Probability Analysis of Successful Cyber Attacks in SDN-based Networks," in *2018 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, 2018, pp. 1-6.

[97] Y. Chen, J. Hong, and C.-C. Liu, "Modeling of intrusion and defense for assessment of cyber security at power substations," *IEEE Transactions on Smart Grid*, vol. 9, pp. 2541-2552, 2016.

[98] "European Union Agency for Cybersecurity (ENISA), Cybersecurity Incident Taxonomy (2018)," *Available at: <https://ec.europa.eu/information_society/newsroom/image/document/2018-*

30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf> [Accessed on: 03/2020].

[99] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *2011 International conference on internet of things and 4th international conference on cyber, physical and social computing*, 2011, pp. 380-388.

[100] T. Fleury, H. Khurana, and V. Welch, "Towards a taxonomy of attacks against energy control systems," in *International Conference on Critical Infrastructure Protection*, 2008, pp. 71-85.

[101] Z. Drias, A. Serhrouchni, and O. Vogel, "Taxonomy of attacks on industrial control protocols," in *2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS)*, 2015, pp. 1-6.

[102] Y. Xiang, L. Wang, and N. Liu, "Coordinated attacks on electric power systems in a cyber-physical environment," *Electric Power Systems Research*, vol. 149, pp. 156-168, 2017.

[103] X. Liu and Z. Li, "False data attack models, impact analyses and defense strategies in the electricity grid," *The Electricity Journal*, vol. 30, pp. 35-42, 2017.

[104] C.-W. Ten, K. Yamashita, Z. Yang, A. V. Vasilakos, and A. Ginter, "Impact assessment of hypothesized cyberattacks on interconnected bulk power systems," *IEEE Transactions on Smart Grid*, vol. 9, pp. 4405-4425, 2017.

[105] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer Networks*, vol. 57, pp. 1344-1371, 2013.

[106] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication

architectures in smart grid," *Computer networks*, vol. 55, pp. 3604-3629, 2011.

[107] A. Zheng, Q. Huang, D. Cai, J. Li, S. Jing, W. Hu, *et al.*, "Quantitative Assessment of Stochastic Property of Network-Induced Time Delay in Smart Substation Cyber Communications," *IEEE Transactions on Smart Grid*, vol. 11, pp. 2407-2416, 2019.

[108] M. A. Aftab, S. S. Hussain, I. Ali, and T. S. Ustun, "IEC 61850 based substation automation system: A survey," *International Journal of Electrical Power & Energy Systems*, vol. 120, p. 106008, 2020.

[109] S. R. Firouzi, L. Vanfretti, A. Ruiz-Alvarez, H. Hooshyar, and F. Mahmood, "Interpreting and implementing IEC 61850-90-5 routed-sampled value and routed-GOOSE protocols for IEEE C37. 118.2 compliant wide-area synchrophasor data transfer," *Electric power systems research*, vol. 144, pp. 255-267, 2017.

[110] B. Moussa, M. Debbabi, and C. Assi, "A detection and mitigation model for PTP delay attack in an IEC 61850 substation," *IEEE Transactions on Smart Grid*, pp. 3954 - 3965, 2016.

[111] J. Zhao, K. Qian, J. Yao, S. Wang, Z. Yang, Z. Gao, *et al.*, "A network scheme for process bus in smart substations without using external synchronization," *International Journal of Electrical Power & Energy Systems*, vol. 64, pp. 579-587, 2015.

[112] L. E. da Silva and D. V. Coury, "A new methodology for real-time detection of attacks in IEC 61850-based systems," *Electric Power Systems Research*, vol. 143, pp. 825-833, 2017.

[113] I.-H. Lim and T. S. Sidhu, "A new local backup scheme considering simultaneous faults of protection IEDs in an IEC 61850-based substation,"

International Journal of Electrical Power & Energy Systems, vol. 77, pp. 151-157, 2016.

[114] S. Lim, "A service interruption free testing methodology for IEDs in IEC 61850-based substation automation systems," *International Journal of Electrical Power & Energy Systems,* vol. 87, pp. 65-76, 2017.

[115] Y. Xiang and L. Wang, "A game-theoretic study of load redistribution attack and defense in power systems," *Electric Power Systems Research,* vol. 151, pp. 12-25, 2017.

[116] H. Lin, A. Slagell, Z. T. Kalbarczyk, P. W. Sauer, and R. K. Iyer, "Runtime semantic security analysis to detect and mitigate control-related attacks in power grids," *IEEE Transactions on Smart Grid,* vol. 9, pp. 163-178, 2016.

[117] J. Wang, L. C. Hui, S.-M. Yiu, E. K. Wang, and J. Fang, "A survey on cyber attacks against nonlinear state estimation in power systems of ubiquitous cities," *Pervasive and Mobile Computing,* vol. 39, pp. 52-64, 2017.

[118] M. Touhiduzzaman, A. Hahn, and A. Srivastava, "A diversity-based substation cyber defense strategy utilizing coloring games," *IEEE Transactions on Smart Grid,* 2018.

[119] Z. Wang, Y. Chen, F. Liu, Y. Xia, and X. Zhang, "Power System Security Under False Data Injection Attacks With Exploitation and Exploration Based on Reinforcement Learning," *IEEE Access,* vol. 6, pp. 48785-48796, 2018.

[120] J. E. Sullivan and D. Kamensky, "How cyber-attacks in Ukraine show the vulnerability of the US power grid," *The Electricity Journal,* vol. 30, pp. 30-35, 2017.

[121] N. Voropai, D. Efimov, I. Kolosok, V. Kurbatsky, A. Glazunova, E. Korkina, *et al.*, "Intelligent control and protection in the Russian electric power system,"

in *Application of Smart Grid Technologies*, ed: Elsevier, 2018, pp. 61-140.

[122] N. Ali, B. M. Ali, M. L. Othman, and K. Abdel-Latif, "Performance of communication networks for Integrity protection systems based on travelling wave with IEC 61850," *International Journal of Electrical Power & Energy Systems*, vol. 95, pp. 664-675, 2018.

[123] A. Chattopadhyay, A. Ukil, D. Jap, and S. Bhasin, "Toward threat of implementation attacks on substation security: Case study on fault detection and isolation," *IEEE Transactions on Industrial Informatics*, vol. 14, pp. 2442-2451, 2017.

[124] M. Zhou, Y. Wang, A. K. Srivastava, Y. Wu, and P. Banerjee, "Ensemble-Based Algorithm for Synchrophasor Data Anomaly Detection," *IEEE Transactions on Smart Grid*, vol. 10, pp. 2979-2988, 2018.

[125] J. Kim and J. Park, "FPGA-based network intrusion detection for IEC 61850-based industrial network," *ICT Express*, vol. 4, pp. 1-5, 2018.

[126] L. Maglaras, M. A. Ferrag, A. Derhab, M. Mukherjee, H. Janicke, and S. Rallis, "Threats, Protection and Attribution of Cyber Attacks on Critical Infrastructures," *arXiv.org preprint arXiv:1901.03899, Cornell University,* 2019.

[127] M. X. Cheng, M. Crow, and Q. Ye, "A game theory approach to vulnerability analysis: Integrating power flows with topological analysis," *International Journal of Electrical Power & Energy Systems,* vol. 82, pp. 29-36, 2016.

[128] P. Eder-Neuhauser, T. Zseby, J. Fabini, and G. Vormayr, "Cyber attack models for smart grid environments," *Sustainable Energy, Grids and Networks*, vol. 12, pp. 10-29, 2017.

[129] D. Ishchenko and R. Nuqui, "Secure communication of intelligent electronic

devices in digital substations," in *2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*, 2018, pp. 1-5.

[130] J. Jarmakiewicz, K. Parobczak, and K. Maślanka, "Cybersecurity protection for power grid control infrastructures," *International Journal of Critical Infrastructure Protection*, vol. 18, pp. 20-33, 2017.

[131] A. Mahor, V. Prasad, and S. Rangnekar, "Economic dispatch using particle swarm optimization: A review," *Renewable and sustainable energy reviews*, vol. 13, pp. 2134-2141, 2009.

[132] S. Krishnamurthy and R. Tzoneva, "Investigation on the impact of the penalty factors over solution of the dispatch optimization problem," in *2013 IEEE International Conference on Industrial Technology (ICIT)*, 2013, pp. 851-860.

[133] J. Kennedy, "Particle swarm optimization," *Encyclopedia of machine learning*, pp. 760-766, 2010.

[134] P. Vu, D. Le, N. Vo, and J. Tlusty, "A novel weight-improved particle swarm optimization algorithm for optimal power flow and economic load dispatch problems," in *IEEE PES T&D 2010*, 2010, pp. 1-7.

[135] N. Singh and Y. Kumar, "Economic load dispatch with environmental emission using MRPSO," in *2013 3rd IEEE International Advance Computing Conference (IACC)*, 2013, pp. 995-999.

[136] K. Dasgupta and S. Banerjee, "An analysis of economic load dispatch using different algorithms," in *2014 1st International Conference on Non Conventional Energy (ICONCE 2014)*, 2014, pp. 216-219.

[137] D. E. Goldberg and J. H. Holland, "Genetic algorithms and machine learning," *Machine learning*, vol. 3, pp. 95-99, 1988.

[138] D. C. Mazur, R. A. Entzminger, and J. A. Kay, "Enhancing traditional process

SCADA and historians for industrial & commercial power systems with energy (Via IEC 61850)," in *IEEE Transactions on Industry Applications, vol. 52, no. 1, pp. 76-82*, 2016, pp. 1-7.

[139] M. El Hariri, E. Harmon, T. Youssef, M. Saleh, H. Habib, and O. Mohammed, "The iec 61850 sampled measured values protocol: Analysis, threat identification, and feasibility of using nn forecasters to detect spoofed packets," *Energies*, vol. 12, p. 3731, 2019.

[140] N. S. Kush, E. Ahmed, M. Branagan, and E. Foo, "Poisoned GOOSE: Exploiting the GOOSE protocol," in *Proceedings of the Twelfth Australasian Information Security Conference (AISC 2014)[Conferences in Research and Practice in Information Technology, Volume 149]*, 2014, pp. 17-22.

[141] S. Hussain, A. Iqbal, S. Zanero, S. S. Hussain, A. Shikfa, E. Ragaini, *et al.*, "A novel methodology to validate cyberattacks and evaluate their impact on power systems using real time digital simulation," in *2021 IEEE Texas Power and Energy Conference (TPEC)*, 2021, pp. 1-6.

[142] S. S. Hussain, T. S. Ustun, and A. Kalam, "A review of IEC 62351 security mechanisms for IEC 61850 message exchanges," *IEEE Transactions on Industrial Informatics*, vol. 16, pp. 5643-5654, 2019.

[143] S. S. M. Reshikeshan, M. B. Koh, and M. S. Illindala, "Rainbow Signature Scheme to Secure GOOSE Communications From Quantum Computer Attacks," *IEEE Transactions on Industry Applications*, vol. 57, pp. 4579-4586, 2021.

[144] T. T. Tesfay and J.-Y. Le Boudec, "Experimental comparison of multicast authentication for wide area monitoring systems," *IEEE Transactions on Smart Grid*, vol. 9, pp. 4394-4404, 2017.

[145] S. M. Farooq, S. S. Hussain, and T. S. Ustun, "Performance evaluation and analysis of IEC 62351-6 probabilistic signature scheme for securing GOOSE messages," *IEEE Access*, vol. 7, pp. 32343-32351, 2019.

[146] "Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850," 1.0. IEC 62351-6:2020, IEC, 2020.

[147] S. S. Hussain, S. M. Farooq, and T. S. Ustun, "Analysis and implementation of message authentication code (MAC) algorithms for GOOSE message security," *IEEE Access*, vol. 7, pp. 80980-80984, 2019.

[148] U. Tefek, E. Esiner, D. Mashima, B. Chen, and Y.-C. Hu, "Caching-based Multicast Message Authentication in Time-critical Industrial Control Systems," in *IEEE INFOCOM 2022-IEEE Conference on Computer Communications*, 2022, pp. 1039-1048.

[149] E. Esiner, U. Tefek, H. S. Erol, D. Mashima, B. Chen, Y.-C. Hu, *et al.*, "LoMoS: Less-Online/More-Offline Signatures for Extremely Time-Critical Systems," *IEEE Transactions on Smart Grid*, vol. 13, pp. 3214-3226, 2022.

[150] J. Hong, R. F. Nuqui, A. Kondabathini, D. Ishchenko, and A. Martin, "Cyber attack resilient distance protection and circuit breaker control for digital substations," *IEEE Transactions on Industrial Informatics*, vol. 15, pp. 4332-4341, 2018.

[151] T. S. Ustun, S. Hussain, A. Ulutas, A. Onen, M. M. Roomi, and D. Mashima, "Machine Learning-Based Intrusion Detection for Achieving Cybersecurity in Smart Grids Using IEC 61850 GOOSE Messages," *Symmetry*, vol. 13, p. 826, 2021.

[152] X. Wang, C. Fidge, G. Nourbakhsh, E. Foo, Z. Jadidi, and C. Li, "Anomaly

Detection for Insider Attacks from Untrusted Intelligent Electronic Devices in Substation Automation Systems," *IEEE Access,* 2022.

[153] L. Yang, Y. Zhai, Y. Zhang, Y. Zhao, Z. Li, and T. Xu, "A new methodology for anomaly detection of attacks in IEC 61850-based substation system," *Journal of Information Security and Applications,* vol. 68, p. 103262, 2022.

[154] S. S. Hussain, T. S. Ustun, and A. Kalam, "A review of IEC 62351 security mechanisms for IEC 61850 message exchanges," *IEEE Transactions on Industrial Informatics,* 2019.

[155] T. S. Ustun, S. S. Hussain, L. Yavuz, and A. Onen, "Artificial Intelligence Based Intrusion Detection System for IEC 61850 Sampled Values Under Symmetric and Asymmetric Faults," *IEEE Access,* vol. 9, pp. 56486-56495, 2021.

[156] M. Rodríguez, J. Lázaro, U. Bidarte, J. Jiménez, and A. Astarloa, "A Fixed-Latency Architecture to Secure GOOSE and Sampled Value Messages in Substation Systems," *IEEE Access,* vol. 9, pp. 51646-51658, 2021.

[157] D. R. Gurusinghe, S. Kariyawasam, and D. S. Ouellette, "Testing of Switchgear Operation in an IEC 61850 based SAS using a Real-Time Simulator," *PAC World Conference,* 2018.

[158] R. Kuffel, J. Giesbrecht, T. Maguire, R. Wierckx, and P. McLaren, "RTDS-a fully digital power system simulator operating in real time," in *Proceedings 1995 International Conference on Energy Management and Power Delivery EMPD'95*, 1995, pp. 498-503.

[159] V. Ndatinya, Z. Xiao, V. R. Manepalli, K. Meng, and Y. Xiao, "Network forensics analysis using Wireshark," *International Journal of Security and Networks,* vol. 10, pp. 91-106, 2015.

[160] C. Devanarayana, "Inline Packet Modifier using Snort, RTDS Technologies," Available at: <https://github.com/chamara84/snort-2.9_RTDS> [Accessed on: 11/2020].

[161] C. Jegues, "Banshee Microgrid Sample Case," *RTDS Technologies,* Nov. 2019.

[162] K. Wang, J. Yu, Y. Yu, Y. Qian, D. Zeng, S. Guo, *et al.*, "A survey on energy internet: Architecture, approach, and emerging technologies," *IEEE Systems Journal,* vol. 12, pp. 2403-2416, 2017.

[163] G. R. Gray, J. Simmins, G. Rajappan, G. Ravikumar, and S. Khaparde, "Making distribution automation work: Smart data is imperative for growth," *IEEE Power and Energy Magazine,* vol. 14, pp. 58-67, 2015.

[164] S. Hussain, J. H. Fernandez, A. K. Al-Ali, and A. Shikfa, "Vulnerabilities and countermeasures in electrical substations," *International Journal of Critical Infrastructure Protection,* p. 100406, 2021.

[165] J. G. Wright and S. D. Wolthusen, "Access Control and Availability Vulnerabilities in the ISO/IEC 61850 Substation Automation Protocol," *Lecture Notes in Computer Science, Springer, Cham,* vol. 10242, 2017.

[166] M. T. A. Rashid, S. Yussof, Y. Yusoff, and R. Ismail, "A review of security attacks on IEC61850 substation automation system network," in *Proceedings of the 6th international conference on information technology and multimedia*, 2014, pp. 5-10.

[167] J. Hoyos, M. Dehus, and T. X. Brown, "Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure," in *2012 IEEE Globecom Workshops*, 2012, pp. 1508-1513.

[168] S. E. Quincozes, C. Albuquerque, D. Passos, and D. Mossé, "A survey on intrusion detection and prevention systems in digital substations," *Computer*

Networks, vol. 184, p. 107679, 2021.

[169] J. Hong, C.-C. Liu, and M. Govindarasu, "Integrated anomaly detection for cyber security of the substations," *IEEE Transactions on Smart Grid,* vol. 5, pp. 1643-1653, 2014.

[170] S. S. Hussain, S. M. Farooq, and T. S. Ustun, "A method for achieving confidentiality and integrity in IEC 61850 GOOSE messages," *IEEE transactions on Power Delivery,* vol. 35, pp. 2565-2567, 2020.

[171] M. El Hariri, S. Faddel, and O. Mohammed, "Physical-model-checking to detect switching-related attacks in power systems," *Sensors,* vol. 18, p. 2478, 2018.

[172] V. K. Singh and M. Govindarasu, "A Cyber-Physical Anomaly Detection for Wide-Area Protection using Machine Learning," *IEEE Transactions on Smart Grid, Early Access,* 2021.

[173] J. Montoya, R. Brandl, K. Vishwanath, J. Johnson, R. Darbali-Zamora, A. Summers, *et al.,* "Advanced laboratory testing methods using real-time simulation and hardware-in-the-loop techniques: a survey of smart grid international research facility network activities," *Energies,* vol. 13, p. 3267, 2020.