Cyber-Physical Attacks Detection and Resilience Methods in Smart Grids

Abdullah Mohamad Sawas

A DISSERTATION SUBMITTED TO
THE FACULTY OF GRADUATE STUDIES
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

Graduate Program in Electrical
Engineering and Computer Science
York University
Toronto, Ontario
September, 2022

Abstract

Backed by the deployment of increasingly reliable Information and Communication Technologies (ICT) infrastructure, modern power systems heavily depend on computerized circuits to function within an interconnected environment. In particular, Smart Grids (SGs) core domain relies on ICTs networks and components to communicate control signals and data measurements to improve the efficiency of power generation and distribution while maintaining safe and reliable operations. ICTs have also extended the SG domain of interaction to include other utilities, such as the natural gas grid to efficiently utilize multiple energy forms and resources. In the consumer domain, a growing number of appliances and autonomous smart loads equipped with Internet of Things (IoT) technology are being deployed into SG, the results in large portions of electric demand being remotely controlled. Despite their advantages, ICTs are vulnerable to cyber–attacks that can deteriorate SGs' operational safety and integrity. Thus, new approaches to enhance the resiliency of SGs against cyber–physical attacks are needed. To that extent, this thesis develops new resiliency investigation approaches under the three aforementioned domains.

First, in the SG domain, an efficient False Data Injection Attack (FDIA) approach is developed imitating an intelligent adversary behavior searching for an optimal attack vector against State Estimation (SE) modules. Simulation results show that using this approach, an adversary can identify attack vectors with minimal size and superior flexibility to manipulate, in real-time, power flow measurements of the system lines as perceived by the SE without the need to acquire additional measurements. Hence, attacks constructed using this approach require less computational time and resources compared to

the existing methods making it beneficial for the analysis of cyber–security vulnerabilities and the design of resilient SE modules.

Second, under the Integrated Energy System (IES) domain, an operational framework model is developed to be used as a testbed for performing and analyzing the impact of cyber–attacks. The framework models steady–state power and gas flow operations, and presents a new financial interdependency operation scheduling model. The framework is validated on standard power distribution and transmission systems with variable generation and demand scenarios and high renewable penetration levels. Using this framework, an attack resiliency method is developed based on signal processing and machine-learning tools. The method is able to detect 98.6% and 94.5% of the external signals and internal control commands respectively.

Third, the vulnerability of Power Distribution Systems (PDSs) to compromised collections of IoT-enabled appliances is investigated, and a stealthy attack strategy is presented. Accordingly, a new index is developed, referred to as Feeder Loading Abnormal Power Spectrum (FLAPS), and used in a novel real-time detection and prediction approach to counter stealthy attacks and estimate the attack onset time. Results demonstrate that the method is able to detect and alert for stealthy attacks in a timely manner, thereby enabling the system to operate reliably and securely.

By identifying new attacks, and proposing detection methods and countermeasures, this thesis contributes to the collective efforts to address the risks associated with cyber–attacks against the SGs components. Specifically, the quantitative results show that deploying the proposed methods will enhance the resiliency of SE and IESs, and protect the PDSs against threats of large-scale deployment of IoT-enabled appliances.

Dedication

To the soul of my father,

to my mother,

my wife; Khadija,

my kids,

my family,

and friends.

Acknowledgments

The journey of earning a doctorate degree and writing a dissertation has been a challenging experience with ups and downs. Without the contribution, assistance, and support from numerous individuals, this journey would not have been successful.

First and foremost, I would like to express my deep and sincere gratitude to my research supervisor, Prof. Hany Farag, for giving me the opportunity to conduct research under his supervision in Smart Grid Lab. His invaluable patience, guidance, and advice carried me through all the stages of my dissertation.

I also could not have undertaken this journey without my doctorate committee members Prof. Natalija Vlajic and Prof. Afshin Rezaei. Thank you for your support and advice throughout the Ph.D. milestones. I would also extend my gratitude to the defense committee members, who generously provided knowledge and expertise. Thanks should also go to the fellow members of the EECS graduate office for their help in formalities and admin support.

I am also grateful to my office mates in Smart Grid Lab, Nader El-Taweel, Mohammad Zaki, Abdullah AlObaidi, Abdulrahman AboMazid, Abdallah Hasan, and Gouri Barai for their moral support and encouragement. I am particularly thankful to Dr. Hadi Khani for the great discussions and for sharing his research experience. My special heartiest thanks to my graduate studies companion, Mahmoud Afifi for always being there.

Last but not least, I wish to acknowledge the support and great love of my parents, my wife, Khadija; and my children. They kept me going on and this work would not have been possible without their encouragement.

Table of Contents

Abstract ii

Dedication iv

Acknowledgments v

Table of Contents vi

List of Tables x

List of Figures xi

List of Acronyms xv

Chapter 1 - Introduction 1

1.1 Motivation 2

1.2 Research Gaps 5

1.3 Thesis Contribution 9

1.4 Thesis Layout 10

Chapter 2 - Literature Survey 12

2.1 Modern Smart Grids 12

2.2 Integrated Energy Systems 15

2.2.1 Joint Operation of PtG–GfG Units 16

2.2.2 Power–to–Gas Technology 18

2.3 Cyber Physical Systems Security Challenges and Countermeasures 21

2.3.1 False Data Injection Attacks 25

2.3.2 IoT-Devices Security in Power Systems Applications 27
2.3.3 IoT Vulnerability 28

Chapter 3 - Two-fold Intelligent Approach for Successful FDI Attack on Power Systems State Estimation 31
3.1 Introduction 32
3.2 Problem Formulation and Preliminaries 33
3.2.1 Nonlinear and Linear State Estimation Models 33
3.2.2 Bad Data Detection (BDD) Approach 36
3.2.3 False Data Injection Attacks 36
3.2.4 Optimal Attack Vectors Formulation 37
3.3 Proposed Two-fold Attack Vector Construction Approach 37
3.3.1 Step1: Identification of Vector Candidates 39
3.3.2 Step2: Modeling Attack Vectors Using ANN 40
3.4 Numerical Results 41
3.4.1 System Model 41
3.4.2 Attack Vector Variables Selection 42
3.4.3 Attack vector Ranking 44
3.4.4 Ramp-up Attack Strategy 45
3.5 Summary and Discussion 46

Chapter 4 - Framework for Evaluating Cyber–Attacks on IPGS 48
4.1 Introduction 48
4.2 Framework Architecture 49
4.3 Integrated System Model 51
4.3.1 Electrical Power System Model 51
4.3.2 Gas Flow in the Natural Gas System 53
4.3.3 Energy Conversion Between the Gas and Power Systems 53
4.3.4 Optimization Formulation 54
4.3.5 Objective Function 56
4.4 Case Studies 57
4.4.1 Case Study 1: Optimal Sizing of PtG Units toward Elevated Renewable Power Penetration 58
4.4.2 Case Study 2: Electricity Pricing Market Impact on IPGS Scheduling 63
4.5 Summary and Discussion 75

Chapter 5 - Develop Intelligent Detection Approach for False Data Injection Attacks against Power and Gas Systems Integration Facilities 77
5.1 Introduction . . . 78
5.2 Problem Description and Hypothesis . . . 79
5.3 Cyber-Attack Detection Model . . . 80
5.3.1 Detecting Attacks on Primary Signals . . . 82
5.3.2 Detecting Attacks on Secondary Signals . . . 86
5.4 Case Studies and Discussion . . . 88
5.4.1 Impact of Attacks on the Facility Operation . . . 88
5.4.2 Aggressive Attacks without Detection Model . . . 92
5.4.3 Secondary Signals Attacks Detection . . . 93
5.4.4 Primary Signals Attacks Detection . . . 96
5.5 Summary and Discussion . . . 99

Chapter 6 - Real-Time Detection of Surreptitious IoT-Based Cyber–attacks in Power Distribution Systems 100
6.1 Introduction . . . 100
6.2 Problem Description . . . 101
6.3 Stealthy Attack Modeling and Mathematical Formulation . . . 103
6.3.1 Adversary and Attack Characteristics . . . 104
6.3.2 Optimal Attack Model . . . 106
6.3.3 Appliance Discomfort Model . . . 108
6.3.4 Smart Appliances Load Model . . . 110
6.3.5 Adversary Power Distribution System Model . . . 113
6.4 Proposed Attack Prediction and Detection Framework . . . 114
6.4.1 Overview of the Proposed Framework . . . 116
6.4.2 Feeder Loading Abnormal Power Spectrum (FLAPS) Index . . . 116
6.4.3 Anomaly Detection via FLAPS Prediction . . . 120
6.5 Case Studies and Discussion . . . 125
6.5.1 Impact on Feeder's Daily Load Curve . . . 126
6.5.2 Impact on a group of houses . . . 126
6.5.3 Impact on bus voltage and LVR operation . . . 127
6.5.4 Attack Detection . . . 128
6.5.5 Attack Onset Time Estimation using Piecewise Regression . . . 130
6.6 Conclusion . . . 131

Chapter 7 - Conclusion and Future Work **133**
7.1 Summary and Conclusions 133
7.2 Future Work 135

Bibliography **137**

Appendices **154**

Appendix A: List of Publications **154**

Appendix B: Attributions **155**

List of Tables

2.1 Comparison between electrolyzer technologies 19

3.1 Optimal Attack Vectors Components Results: target state active power flow measurements in lines #12, #8 and #15 42

4.1 Wholesale electricity price analysis 75

5.1 Simulation and Modeling Parameters 90
5.2 Probability Distribution of Operation Mode Classes 95
5.3 Results from Comparing the Accuracy of the Proposed Scheme on Detecting the FDIA on Primary Signals with Prior Machine-Learning Schemes. . 97
5.4 Accuracy of Detecting FDIA at Different Number of Attacked Samples and Training Data With/Without Noise. 98

6.1 Adversary Model Characteristics 104
6.2 Attack Model Characteristics 106
6.3 The results of attack onset time estimation for attacks started at 5:00 am . 131

List of Figures

1.1 Overlay of the resiliency methods developed in this thesis for Smart Grids. 4

2.1 Basic Structure of the Electric Power Distribution System 13
2.2 Schematic of integrated power and natural gas system. 16
2.3 The steps of power-to-gas process. 18
2.4 Typical CPS structure 21
2.5 Type of attacks targeting CPSs based on the location of the attack. 22
2.6 The structure of a typical IoT-enabled device communication with the cloud-based services. 28
2.7 Types of the physical impact of cyber–physical attacks on Smart Home Energy Management Systems (SHEMSs). 30

3.1 Placement of metering units on the IEEE-14 Bus System 34
3.2 Flowchart of the proposed two-fold method to construct optimal attack vectors. 38
3.3 Minimum attack vector size to perform successful FDIA targeting lines' active power flow. 43
3.4 The rank of two attack vectors #1 and #2 according to their probability of performing successful FDIAs. 44
3.5 Average SSE under two ANN-modeled attack vectors #1 and #2 target gradual change in the line power flow. 45
3.6 Comparing system state variables for two attack vectors #1 and #2 that target gradual change in the line power flow. 47

4.1 Framework steps for analyzing cyber–physical security of integrated power and gas systems 49
4.2 Screenshot of the main interface of the IPGS framework. 50
4.3 IPGS power results panel 51

4.4 IPGS steady-state results panel 52
4.5 The impact of PtG unit size (MW) on (a) Average yearly utilization (%), (b) Renewable energy penetration (%), and (c) Arbitrage revenue of the facility. 60
4.6 Monthly operation results of the facility at optimal PtG size (32 MW) and $c^{\text{Ren}} = 1500$ illustrating (a) PtG operation, (b) Available renewable energy and system's energy demand, and (c) Arbitrage revenue and average electricity price. 62
4.7 Embedded power and natural gas distribution system. 64
4.8 System operating parameters under real-time and ToU price scheduling schemes: (a) Power generation under real-time pricing, (b) Power demand under real-time, (c) Power generation under ToU pricing, and (d) Power demand under ToU pricing. 66
4.9 Monthly operation of GfG and PtG units for the studied year: *(a)* Under real-time pricing scheme, and *(b)* Under ToU pricing scheme. 67
4.10 Voltage analysis of the 33 buses in the system under real-time and ToU pricing schemes:*(a)* Probability density function (PDF), *(b)* Voltage mean value, and *(c)* Voltage standard deviation. 68
4.11 Gas grid pressure and flow analysis under real-time and ToU pricing schemes: *(a)* Pressure probability density function, and *(b)* Flow probability density function. 69
4.12 Comparing revenue and cost analysis under real-time and ToU pricing schemes: (a) Arbitrage revenue without renewable curtailment, (b) Arbitrage revenue with renewable curtailment, (c) Power losses, and (d) Curtailed power 70
4.13 Operating parameters with GfG unit only under real-time and ToU scheduling schemes: *(a)* GfG output power, *(b)* Arbitrage revenue, and *(c)* Power loss cost 72
4.14 Operating parameters with PtG unit only under real-time and ToU scheduling schemes: *(a)* PtG input power, *(b)* Arbitrage revenue, and *(c)* Power loss cost. 73

5.1 Framework for development of cyber–attack resilient scheduling model in an integrated power and gas transmission system. 79
5.2 Flowchart of the IPGS signals verification model 81

5.3 Flowchart of primary signals verification. 83
5.4 Compound primary signals: (a) Normalized values, (b) Frequency components acquired using CWT. 84
5.5 Verifying secondary signals received from the central controller. 87
5.6 30–bus IEEE-standard power transmission system integrated with a 20–node gas transmission grid employed for numerical studies. 89
5.7 Monthly operating of PtG/GfG facilities: (a) Base generation, (b) GfG generation, (c) PtG demand, (d) Arbitrage revenue, and (e) Lines capacity violation. 91
5.8 Transmission lines capacity violations during aggressive cyber–attacks without the utilization of a verification model. 93
5.9 Actual and estimated operation of (a) PtG and (c) GfG units using the proposed C+RegNN compared with RegNN and NARX models; Error in estimation is compared in (b) for PtG and (d) for GfG units. 94
5.10 Precision percentage versus absolute estimation error of (a) PtG and (b) GfG, unit setpoints using RegNN and C+RegNN models. 96

6.1 Flowchart: a potential scenario to compromise set of IoT-devices. 102
6.2 Schematic of the attack model on PDSs via compromised IoT-enabled appliances. 107
6.3 One day profile of (a) The power consumption signal of an AC, and (b) the associated indoor temperature and setpoint signals. 112
6.4 Radial feeder in a PDS. 113
6.5 The proposed anomaly prediction and detection framework. 115
6.6 Flowchart of the steps to calculate the proposed FLAPS index. 119
6.7 Left: the unfolded LSTM neural network model structure consists of interlinked LSTM cells in the hidden layers; Right: LSTM cell's inner structure. 121
6.8 Three multi-step prediction approaches: (A) single-model recursive one-step, (B) multi-model recursive one-step, and (C) single-model multi-steps. 123
6.9 Feeder's load duration curve during normal and attack scenarios. 126
6.10 One day profile for a group of adjacent houses with compromised Air Conditioner (AC) units: (a) The aggregated power demand, and (b) manipulated temperature setpoint vs. outdoor temperature. 127

6.11 (a) Bus-680 voltage profile during normal and attack scenarios, and (b) Relative increase of LVR operation vs. percentage of compromised IoT-enabled appliances. 128
6.12 FLAPS index curve during normal and different attack severity conditions. 129
6.13 Attack onset time estimation. Top: the FLAPS curve segments Γ^{S_1} and Γ^{S_2} before and after the attack, respectively. Bottom: least-square fitting errors. 131

List of Acronyms

AC Air Conditioner. xiii, 109, 111, 126, 127
AEL Alkaline Electrolyzer. 18, 19
AGC Automatic Generation Control. 5
AMI Advanced Metering Infrastructure. 5
ANN Artificial Neural Network. 32, 39, 40, 45, 96, 98

BDD Bad Data Detection. 5, 6, 9, 10, 26, 31, 32, 36, 39, 44, 45, 90, 97, 133
BTM behind-the-meter. 100, 104

CNN Convolutional Neural Network. 77, 82, 83, 85, 96, 98
CPS Cyber-Physical System. 1–3, 6, 7, 10, 12, 21, 23, 25, 29
CWT Continuous Wavelet Transform. 82–84

DBN Deep Belief Network. 25
DER Distributed Energy Resource. 136
DoS Denial of Service. 22

ESS Energy Storage System. 14, 16
EV Electric Vehicle. 29

FDIA False Data Injection Attack. ii, x, xi, 4–7, 9–12, 21–27, 30–33, 37, 43, 46, 77–79, 88, 96–98, 133
FLAPS Feeder Loading Abnormal Power Spectrum. iii, xiv, 101, 116, 120–122, 124, 125, 129–131, 134

GA Genetic Algorithm. 31, 32, 37, 39, 42, 46
GfG Gas–fired Generation. 15–17, 49–51, 53–59, 61, 63–65, 67–73, 75–77, 79, 80, 82, 83, 86–88, 90, 92, 93, 95, 99

HMC Hourly Maintenance Cost. 88

HVAC Heating, Ventilating and Air Conditioning. 29

ICT Information and Communication Technologies. ii, 1, 2, 6, 12, 21, 78, 135
IED Intelligent Electronic Device. 15
IES Integrated Energy System. iii, 2, 3, 6, 15, 134
IESO Independent Electrical System Operator. 20, 61
IoT Internet of Things. ii, iii, 2, 4, 7–9, 11, 27–29, 100–106, 108–110, 113, 114, 126–128, 131, 133, 134, 136
IPGS Integrated Power and Gas System. 4, 6, 7, 9–12, 25, 48, 58, 75, 133, 135
IQR interquartile range. 74

LDC Local Distribution Company. 57
LSTM Long Short-Term Memory. 8, 101, 116, 120, 121, 134
LVR Line Voltage Regulator. 114, 125–128, 134

MAE Mean Absolute Error. 118, 124
MAPE Mean Absolute Percentage Error. 124
MLE Maximum Likelihood Estimation. 125
MLP Multilayer Perceptron. 40, 41, 46
MTTD Mean Time to Detection. 120

NARX Nonlinear Auto-Regressive model with eXogenous input. 95
NIST National Institute of Standards and Technology. 7

PDF Probability Distribution Function. 68, 70
PDS Power Distribution System. iii, 4, 7–11, 100, 101, 103–106, 108, 110, 113, 114, 116, 117, 127, 128, 131–134, 136
PEM Polymer Electrolyte Membrane. 18–20
PID Proportional-Integral-Derivative. 25
PMU Phasor Measurement Unit. 5, 26
PtG Power–to–Gas. 10, 12, 15–18, 20, 49–51, 54–59, 61, 63–65, 67, 70, 71, 75–77, 79, 80, 82, 83, 86–88, 90, 92, 93, 95, 99
PV Photovoltaic. 13, 49, 82, 88, 90, 96–99

RNN Recurrent Neural Network. 25, 120

SCADA Supervisory Control and Data Acquisition. 4, 9, 14, 15, 30, 133
SE State Estimation. ii, iii, 4–6, 9, 10, 15, 24, 31, 33, 35–37, 39, 41, 44, 46, 133–135

SG Smart Grid. ii, iii, 1, 3–7, 9, 10, 12, 14, 21, 23, 29, 133, 135, 136
SHEMS Smart Home Energy Management System. xi, 29, 30
SNG Synthetic Natural Gas. 18, 57
SOEC Solid Oxide Electrolysis Cell. 18, 19
SSE Sum of Squared Errors. 44
SVM Support Vector Machine. 25, 96, 98

ToU Time–of–Use. 57, 58, 63–65, 67–74, 76

WLS Weighted Least Square. 35

Chapter 1

Introduction

The incremental deployment of Cyber-Physical Systems (CPSs) is fundamentally reshaping our modern societies. CPSs encompass computing devices connected to a network of sensors and actuators to control physical systems and processes. Critical and non-critical sectors worldwide rely on CPSs to coordinate and integrate heterogeneous components with intelligent, interactive, and distributed operations. For example, in the healthcare industry connected body sensors allow doctors to monitor patient's vitals in real-time. This continuous monitoring has numerous benefits, such as improved diagnosis, early disease detection, and reduced infection risks. Doctors can use this information to provide better patient care. In intelligent transportation systems, involving connected and autonomous vehicles, traffic congestion can be reduced and road safety improved. The next industrial revolution (i.e., Industry 4.0) will also rely on massive connectivity at scale for process automation. Beyond these examples, CPS introduced improvements to many other industries, including crowd management, public safety, agriculture, and retail.

On one hand, Smart Grid (SG) in power systems is a complex CPS that has been going through major transformations over the past decades. SG utilizes wired/wireless connectivity of smart meters and field devices to improve power generation and distribution [1, 2]. Likewise, utilizing these unprecedented capabilities of Information and Communication Technologies (ICT) backbone, other energy utilities are moving forward

into the deployment of Integrated Energy Systems (IESs). Alongside the advancements in energy generation, conversion, and storage technologies, ICTs have facilitated efficiently combining multiple energy forms and resources within one system [3]. On the other hand, end consumers in recent years have joined the energy efficiency quest by adopting smart homes that entail large-scale deployment of smart appliances, vehicles, and many other smart objects connected to the communication infrastructure through the Internet of Things (IoT) technology. Such ubiquitous, diverse, and massive connectivity is essential for smart world automation systems speculated to improve almost every aspect in our lives [4].

1.1 Motivation

CPSs have many advantages, but their complexity and heterogeneity have also made them susceptible to a wide variety of security and resiliency threats [5]. Attackers have been able to exploit known and zero-day vulnerabilities leading to extensive damages to the targeted CPSs. For example, the Iranian nuclear reactors were hit by Stuxnet malicious worm causing delays in their production rate for years before it was discovered [6, 7]. Another recent attack targeted the Ukrainian power utility and caused blackouts in parts of the national grid [8].

Many efforts have been made to improve CPSs security against cyber–attacks since they were first highlighted, and while many attacks have been successfully blocked, there are still vulnerabilities that attackers can exploit. A careful review of the CPSs security challenges identifies the following two main root causes of vulnerabilities. Firstly, the uncertainty associated with the penetration of new technologies and energy resources is altering the characteristics of conventional physical systems and hence complicating the detection of undesired militant physical behaviors. Secondly, the integration of ICT into the physical system exposes CPSs to a stream of cyber–threats that present additional challenges to its security and resiliency [9]. As a result, substantial research and invest-

ments on security designs and upgrades against unforeseen patterns and threats from cyberspace are indispensable to the safe operation of general CPSs and specifically, their realization in power and energy systems [10].

Unlike the research on cyber–security in the information technology field, addressing the security challenges of CPSs requires a holistic analysis of the security issues considering both the cyber and physical layers and their interaction [10, 11]. IESs further extends this task to considering the integration between multiple energy systems. In a nutshell, the following research methodology is followed in this thesis for the development of new approaches that target enhancing the resiliency of SGs and IES:

1. Develop physical operational models of the underlined SGs system and particular components. The models are utilized as testbeds to study the impact of cyber–physical attacks.

2. Identify the vulnerabilities in the SGs components that can be exploited by intelligent adversaries. The set of required knowledge and capabilities acquainted by the adversaries is discussed.

3. Introduce new cyber–attack scenarios that target the operation of the SG and the interdependency between its components or other integrated resources.

4. Analyze the operational stability and economic impacts of the introduced attack scenarios on the SG using the developed testbed models.

5. Propose defense mechanisms to detect and mitigate the cyber–physical attacks.

6. Analyze the effectiveness of the proposed defense mechanisms under the various attack scenarios.

This thesis contributes to the collective research efforts to enhance the resiliency of SGs against cyber–attacks by proposing solutions to mitigate the cyber–physical security challenges of SGs. Specifically, the methodologies developed in this thesis are grouped

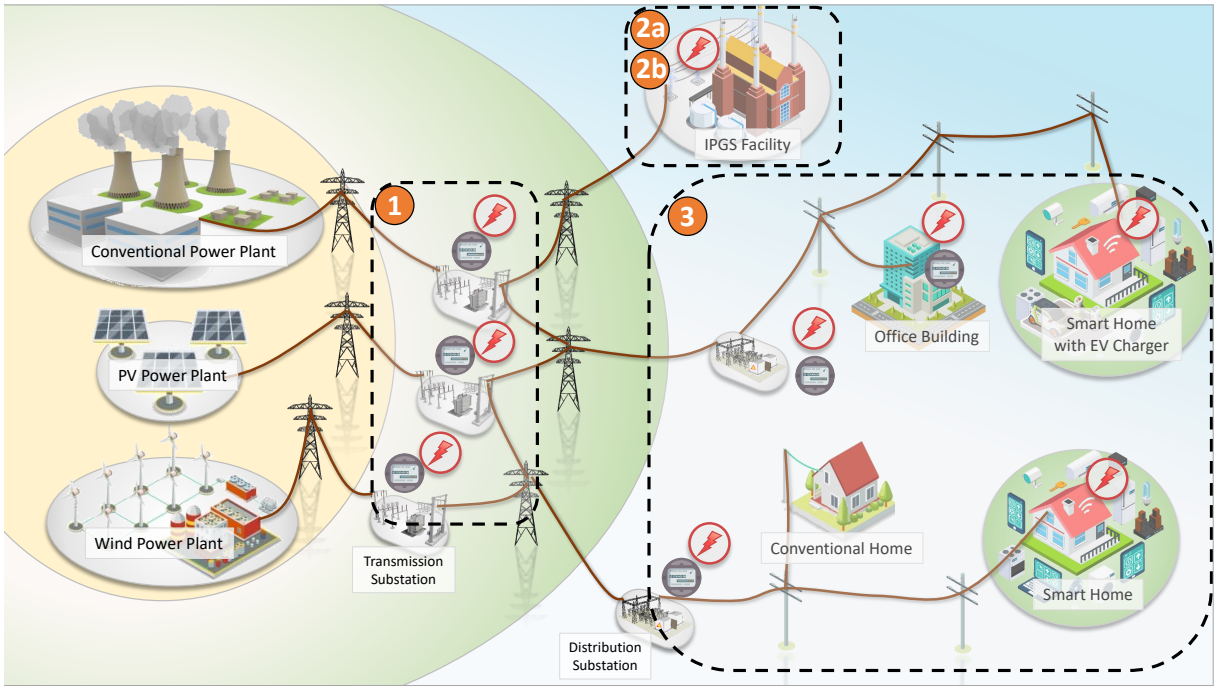


Figure 1.1: Overlay of the resiliency methods developed in this thesis for Smart Grids.

under three main domains related to SGs as shown in the overlay in Figure 1.1. The first domain studies the vulnerability of State Estimation (SE) module that is part of the system's core operation and control scheme, Supervisory Control and Data Acquisition (SCADA). Under this domain, (1) a novel False Data Injection Attack (FDIA) approach is developed to construct attack vectors that target the measurements received by the SE module as the first step to disrupt the integrity of the system. The second domain investigates the resiliency of the integration facilities in Integrated Power and Gas System (IPGS) against cyber–attacks. As such, an operational framework model of the IPGS is developed in (2a) that is utilized as a testbed to benchmark the impact of cyber–attack. Then, in (2b) an attack detection and mitigation method against integration facilities in IPGSs is developed. The third domain concerns the vulnerability of Power Distribution Systems (PDSs) to cyber–attacks that compromise a set of IoT-enabled loads, thereby impacting their efficiency and reliability. As such, a stealthy attack strategy is presented in (3) along with novel real-time anomaly detection and prediction method.

1.2 Research Gaps

In the context of cyber–physical security challenges of SGs, several studies in the literature investigate attacks on a list of SG's components. The list includes subsystems such as Automatic Generation Controls (AGCs), SE, transmission lines, substations, Phasor Measurement Units (PMUs), network topology, circuit breakers, loads, Advanced Metering Infrastructures (AMIs), and electricity markets [12–22]. In particular, a variant of data integrity attack schemes known as FDIA. Here, the adversary intercepts and carefully manipulates the communicated data in order to deceive the operator into issuing the wrong actions. In SG, the attacker performs FDIAs to mislead the system's SE mechanism by manipulating a set of measurements in a way that corrupted data passes basic Bad Data Detection (BDD) checks resulting in wrong statuses getting transmitted to the controller [17]. It has been shown in the literature that conducting successful FDIA is challenging for attackers since it involves (i) finding the optimal attack vector with the least number of measurements to compromise, (ii) collecting the least amount of information about the system; and (iii) sensing and/or masking the post-attack effects [18, 19].

Nevertheless, studies have shown that it is discouraged to rely only on the difficulty of constructing attack vectors to protect the system against FDIAs since attackers are eventually able to outperform these challenges. For instance, the research in [17] proposes an attack vector constructed utilizing a linear model of the system. The work in [23] extended the method to nonlinear system models by relaxation to the original problem and utilizing assumptions to the status vector around the operating point. The study in [24] shows that attackers can perform FDIA with inaccurate information about part of the system while the study in [19] shows that FDIAs can be performed without full information of the entire power network. It is argued that in order to build a successful FDIA on nonlinear SE models, the attacker needs to have information concerning operating conditions [25].

However, still there are some aspects within the existing research for constructing FDIA vectors against SE that have not been well explored in the literature. Firstly, the

works on FDIA have been focused on proposing mitigation countermeasures for simple attacks while neglecting the sophisticated attack techniques that can bypass the proposed countermeasures. Mostly, the attacks presented are derived from simplified linear models of the system utilizing analytical approaches. While attackers nowadays are able to utilize heuristic and machine learning-based intelligent approaches to construct optimal attack vectors, thereby overcoming the complexity of nonlinear models. Additionally, solving analytical methods in real-time requires high-performance computing power that is not usually available to the adversary. Utilizing a machine-learning technique that is trained offline can overcome this limitation in computing resources.

Therefore, to fill these gaps, a FDIA approach is developed imitating an intelligent adversary behavior seeking an optimal attack vector against nonlinear SE modules. The method involves an offline phase to identify the optimal attack vector and an online deployment phase that exploits the real-time values of a particular measurement. During the offline phase, the developed method identifies a set of attack vectors with the lowest number of false measurements to be injected and the low risk of getting detected, i.e., triggering BDD defense mechanisms. A model of the attack is developed using a neural network trained to be deployed during the online phase to perform the attack. By utilizing the neural network the developed method minimizes the amount of information required to be acquainted, thereby reducing the computational time and resources required by the attacker in the online phase.

Across SGs, the vulnerability of IESs to cyber–attacks is also investigated in this thesis. Precisely, the developed research work aims to enhance the resiliency of IPGS facilities against FDIAs on both the input-data and control commands signals. The idea of integrating power and gas energy resources has been widely discussed in the literature from operational and economical perspectives mainly to increase the overall efficiency, operational flexibility, and reliability of the energy systems [26–31]. Being a CPS, IPGSs are also vulnerable to cyber–attacks issues through the ICT layers and components [9]. Nonetheless, prior studies did not investigate these issues and the existing optimal

scheduling models for IPGSs are not tested against cyber–attacks in order to evaluate their resiliency. In fact, prior studies make a strong assumption that input and output data are protected against cyber–attacks by following the cyber–security requirements of standard IT systems. While it is true that principal security requirements of the CPSs should follow standard practices relevant to securing IT systems, the requirements prescribed in the National Institute of Standards and Technology (NIST) framework [32] call for additional measures. Among the actions suggested in this framework is the development and deployment of methods for detecting and monitoring anomalous behavior are mandated. As such, there is a need for new anomaly detection methods for the data and information exchange in IPGSs in order to address their vulnerability to cyber–attacks.

To fill these gaps, first, a framework of the operational model of IPGSs integration facilities is developed to conduct cyber–attack scenarios and evaluate their impacts on both systems. The framework studies the optimal scheduling of the integration units and the deviation in operation during attacks. Second, this framework is utilized to develop anomaly detection methods for the data and control signals communicated internally within the facility and externally from power systems and gas network. By utilizing data forecasting approaches, signal estimation models, and data classification tools, the input/output data are validated considering not only the operational limits but also the physical system constraints. Therefore, implementing the proposed methods will enhance the cyber–attack resiliency of the integration facilities by switching their operating model to internally estimated once FDIAs are detected.

Lastly, the vulnerability of PDS to cyber–attacks via compromising IoT–enabled loads is investigated in the third domain of this work. Unlike utility managed cyber–infrastructure in SGs, the IoT-enabled appliances bring their own challenges [33–36]. When these devices are not properly secured, they can be exploited by unauthorized individuals, which leads to a number of negative consequences. The potential risks associated with unsecured IoT-enabled loads stem from: (i) IoT are deployed by the end customers within their premises, i.e., behind the meter. Such a setup makes no room for utilities

to have direct control over these devices; (ii) Utilities are oblivious to the exact location, specifications, and installation details of these devices hence it is difficult to assess and address their vulnerabilities; and (iii) Although these devices individually do not pose major threats, their coordinated actions may induce significant disturbances to the PDS.

Many research works in the literature have investigated the implications of a compromised group of IoT-enabled loads, however, there is still room for exploring variations of the problem. For instance, a large body of research works focused on the type of attacks that cause disruptions in the system states such as destabilizing the grid frequency, leading to blackouts [37–39], while attacks of stealthy nature are neglected under the impression that they are less severe. Peculiarly, in stealthy attack type, attackers manipulate the data over a long period of time which impacts the PDS equipment life-time and degrades the power quality [40]. Moreover, the aforementioned studies focus on attack mitigation and countermeasures, while the issue of detecting the attack onset time has been overlooked [41]. Nonetheless, detection of the attack is critical to effectively activate defense actions in a timely manner. This is especially important during stealthy attacks to avoid or at least minimize damages to the equipment and quality of service. Last, accurate models of the IoT–enabled appliances that consider their physical and operational constraints with regards to energy consumption and operation dynamics are missed from the existing studies. These models are important when studying real stealthy cyber–attack scenarios against IoT–enabled appliances.

As such, a realistic stealthy attack strategy is presented that minimizes the detection chances while preserving the compromised IoT-enabled appliances operating within the normal ranges. Accordingly, a real-time anomaly detection and prediction method is developed based on demand power spectrum analysis and Long Short-Term Memory (LSTM) neural networks. The attack onset time is estimated and reported to the PDS's operator for post-attack actions. Deploying this method allows for detection and alert for stealthy attacks in a timely manner, thereby enabling the system to operate reliably and securely.

1.3 Thesis Contribution

This thesis develops new cyber–attack detection and resiliency approaches under the three aforementioned domains. A summary of the thesis contributions is presented below:

1. An efficient FDIA approach is developed for SGs that imitates an intelligent adversary behavior searching for an optimal attack vector against SE module that serves as the core of SCADA system.

2. The approach is able to find minimal attack vectors of size 3 that an adversary can successfully compromise to bypass the BDD. It also identifies successful attack vectors that work in real-time during a change between -100% to +100% in the standard system loading without the need to acquire additional measurements.

3. Attacks constructed using this approach require less computational time and resources by the adversary compared to the existing methods making it suitable for generating attacks utilized for the analysis of cyber–security vulnerabilities and design of resilient SE module.

4. A framework is developed to be utilized as a testbed for performing and analyzing the impact of cyber–attacks against IPGS.

5. The framework models steady–state power and gas flow operations, and presents a new financial interdependency operation, and scheduling model.

6. Using this framework, attack detection, and mitigation method is developed based on signal processing and machine-learning tools.

7. The vulnerability and impacts of PDSs to organized cyber–attacks are investigated via compromised IoT-enabled loads.

8. A stealthy attack strategy is presented that minimizes detection chances by reducing the discomfort experienced by the consumers due to abnormal operation of the compromised appliances.

9. A novel real-time anomaly detection and prediction method is proposed based on a machine-learning forecasting tool to detect stealthy attacks.

10. A new index is proposed and utilized to estimate the attack onset time, which is then reported to the PDS's operator for further investigation and action.

11. The proposed technique enhances the resiliency of the PDS via timely detection and alerting for stealthy attacks, thereby enabling the system to operate reliably and securely.

1.4 Thesis Layout

The remainder of this thesis is organized into the following chapters:

- **Chapter 2**: Presents background on modern SGs and their major components and introduces IPGSs with the emerging Power–to–Gas (PtG) technologies. Subsequently, an overview of CPSs is presented with a discussion of the cyber–security challenges and countermeasures. The chapter concludes with a literature survey of FDIA strategies that have been utilized against SGs.

- **Chapter 3**: Introduces an intelligent two-folds approach to optimally construct FDIA vectors against SE. The optimality of the vector is determined in terms of the number of compromised measurements and flexibility of the vector to successfully pass BDD during various network loading conditions. The performance of the produced vectors is analyzed on the IEEE 14-bus system.

- **Chapter 4**: Presents a framework that builds on the interdependency steady-state operation model of the power and gas systems. Case studies to validate the framework are presented considering the optimal sizing of PtG units and the impact of electricity pricing schemes on units scheduling with the presence of renewable resources.

- **Chapter 5**: Presents practical FDIAs models against IPGS integration facilities followed by two novel detection schemes to enhance the resiliency of the facility scheduler. In the first scheme, a supervised machine-learning model is utilized to detect attacks on the information received by the facility scheduler. In the second scheme, an unsupervised hybrid neural network is developed to detect attacks on the output control signals issued by the scheduler. The chapter concludes with case studies to demonstrate the efficacy and feasibility of the proposed models.

- **Chapter 6**: Presents a stealth attack model against PDSs using a set of compromised IoT–enabled appliances. Afterward, novel real-time attack detection and onset time estimation approaches are proposed to counter the stealthy attacks utilizing a new anomaly measurement index. The chapter concludes with impact analysis of the attacks and an evaluation of the detection method using the IEEE-13 bus system model.

- **Chapter 7**: Summarizes the contribution of this thesis in relation to the target research gaps, and expands on the intention to pursue further work in these areas.

Chapter 2

Literature Survey

Modern Smart Grids (SGs) evolved from the traditional power systems with the adoption of Information and Communication Technologies (ICT) infrastructure. This chapter provides a background of key concepts in SGs and their major components. Subsequently, it introduces the operational concept of Integrated Power and Gas Systems (IPGSs) along with the emerging Power–to–Gas (PtG) technologies. Afterward, an overview of Cyber-Physical Systems (CPSs) is presented with a discussion of the cyber–security challenges and countermeasures. The chapter concludes with a literature survey of False Data Injection Attack (FDIA) strategies that have been utilized against SGs.

2.1 Modern Smart Grids

Power systems are complex systems designed and operated to generate, transmit and distribute electrical power to consumers over large geographical areas [42]. Conventionally, as shown in Figure 2.1, the power is generated by generator machines housed in the generation plants, transmitted via subsequent high-voltage transmission lines, and distributed via medium-voltage distribution networks to regular customers [43]. However, over the past decades, the electrical power industry is undergoing rapid and massive transformations mainly due to several factors such as technological development, energy costs

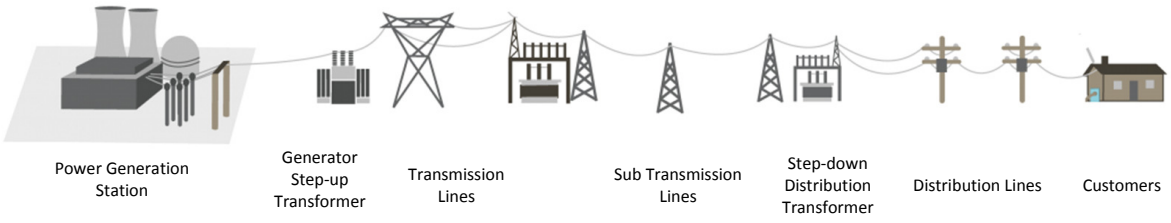


Figure 2.1: Basic Structure of the Electric Power Distribution System

increase, load growth, advancements in communication technology, and climate change concerns [44].

Conventional generators mainly convert mechanical, chemical, or nuclear energy into electrical energy. Most power generation stations operate by burning non-renewable fuel to generate thermal energy that is used to heat water tanks to generate steam. The steam, in turn, propels turbine blades that drive an electric generator, which produces electricity. The process of burning non-renewable fuel releases carbon dioxide into the atmosphere, which contributes to global climate changes [45].

Alternatively, renewable and clean power generation technologies have been introduced as environmentally friendly resources that will play an important role in future power supply. That is due to increased global public awareness of the need for environmental protection and the desire for less dependence on fossil fuels for energy production [46]. Environmentally friendly technologies include power generation from renewable energy resources, such as Photovoltaic (PV), wind, biomass, geothermal [47], micro-hydro, ocean wave and tides, and clean alternative energy power generation technologies such as fuel cells [48] and micro-turbines [46]. Fostered by the advancement in renewable and clean energy technologies on one hand and the possibility of deferring conventional infrastructure upgrades, on the other hand, the penetration of distributed generation units near the customer loads is one of the major transforms in the conventional power systems [49–51].

Several challenges were introduced with the introduction of distributed energy resources which has changed the legacy infrastructure of power systems from being passive systems with unidirectional power flow to active networks with bidirectional power flow. Additionally, the intermittent nature of the renewable and clean energy resources presents challenges for the operation and control of the power grid [52]. Ultimately, having a flexible power system that can maintain the balance between instantaneous electrical power supply and demand is required. This goal can be achieved by integrating various technologies currently available such as dynamic operation and control of conventional generation resources and the power flow in the electricity grid, penetration of energy storage, implementation of demand response programs, and curtailment of the intermittent energy sources. Each of these flexibility options has important advantages and disadvantages in terms of cost and efficiency.

Extensive research work has been conducted on the penetration of renewable energy resources to improve the overall system performance. Hybrid systems i.e., combinations of two or more power generation technologies along with/without a storage system, were also studied for better operational performance, and dispatch and operation control [53–56]. Also, previous studies explored the utilization of different technologies and generation unit sizing in the design of hybrid systems [57], [58].

Energy Storage System (ESS) have been widely integrated within hybrid power generation systems to increase the adoption of intermittent renewable resources [59]. In addition, ESSs can help in maintaining the uninterruptible power supply to critical loads and provide power quality services to power distribution systems [60], [61]. It is noteworthy that several storage technologies vary in capacity, size, response time, and storage lifetime.

Furthermore, this transformation of power systems is accompanied by incremental integration of cyber–enabled devices creating what so-called SGs. This paradigm shift is promising to add several improvements to the flexibility, reliability, and efficiency of grid operations. In particular, Supervisory Control and Data Acquisition (SCADA) is

one of the early applications that evolved with the vast deployment of communication infrastructure. SCADA systems allow power system control centers to collect real-time data from substation Intelligent Electronic Devices (IEDs), control circuit breakers and permit management of the power system from a central location [62]. The data is then continuously analyzed using tools such as *State Estimation (SE)* to assist system operators in making control decisions to preserve the operational constraints of the network hence ensuring power supply security.

2.2 Integrated Energy Systems

Enhancements in energy utilization and distribution have been fueling the plans to incorporate more efficient and less pollutant energy systems. One of the recently investigated options is to integrate multiple energy carrier systems to increase the overall efficiency, operational flexibility, and reliability of the energy systems [26]. Integrated Energy Systems (IESs), also known as multi-carrier energy systems, hybrid energy systems, or energy hubs, incorporate the development and operation of various energy systems, such as electricity, heating, and cooling, gas, transportation, water, renewable energy, and information systems [27].

The unidirectional interdependency between power and gas systems has been extensively investigated in the literature [28–31] focusing on optimizing the allocation and the planning of Gas–fired Generation (GfG) resources. The optimization considers the operational constraints that primarily prevent shortages in power and gas supply while minimizing the associated costs. Additionally, the PtG energy conversion technology has recently gained enormous interest by researchers as an option to alleviate the utilization of renewable energy resources and facilitate seamless adoption for bidirectional integrated systems [63]. PtG technologies convert electricity into another form of valuable energy i.e., hydrogen, that can be either stored or transported to another location via gas transportation systems. A background on the operation principle of PtG process is presented

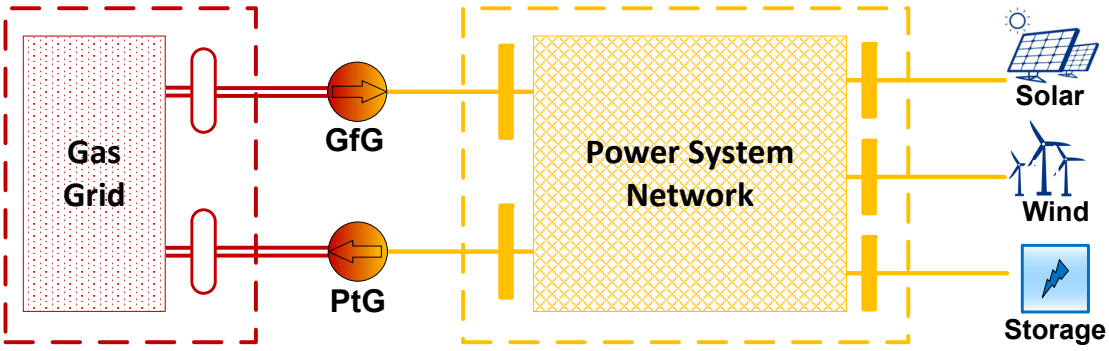


Figure 2.2: Schematic of integrated power and natural gas system.

in Section 2.2.2.

In the research works [64–66], instead of curtailing the excessive electric energy generated by the intermittent renewable resources, the PtG technology was utilized to absorb the surplus energy to maintain a balanced power system grid. The studies in [67, 68] investigated the modeling and scheduling of the PtG plants considering the uncertainty associated with the vast majority of renewable resources and energy demand. As such, technologies to store and convert electricity into another reusable energy form are increasingly being adopted as an effective solution to overcome the intermittency in electricity production associated with renewables [69].

2.2.1 Joint Operation of PtG–GfG Units

A combination of the PtG and GfG units can create a new configuration for bidirectional energy conversion opportunities within integrated gas and power grids. The schematic of such integration is shown in Figure 2.2. An integrated PtG–GfG facility can act as a large-scale ESS with the following advantages:

- **Virtually unlimited capacity:** Unlike conventional electric storage systems, which have specific energy storage capacity, the main advantage of the PtG–GfG facility in an integrated power and gas gird is the superiority to absorb as much surplus

energy as available without inherent capacity limitations. Practically, the amount of energy absorbed is limited by the operational constraints of the gas grids and the power grid, which are very high.

- **State of charge:** PtG–GfG facility does not require absorbing energy from the grid before delivering it back to the grid. The outflow phase occurs when the gas generators in the PtG–GfG facility consume gas to produce electric energy injected into the power system grid. This process depends only on the availability of gas supply, i.e., not on the amounts of electrical energy inflow. The facility can start delivering power even before it absorbs any electrical energy from the grid.

- **Increase in renewable penetration:** The unprecedented increase in renewable energy deployment makes maintaining a balanced power system network challenging. Mainly, this can be contributed to the uncertainty involved with the vast majority of renewable resources being weather dependent such as wind and solar energy [70]. The joint operation of PtG and GfG units can increase the renewable penetration levels by minimizing the adverse impacts of the sporadic energy injection on the power system.

- **Price arbitrage:** the PtG and GfG units can be used to exploit the energy price arbitrage opportunities available in the gas and electricity prices.

- **Ancillary services:** the joint operation of the PtG and GfG units can offer ancillary services to the grid such as resolving congestion issues in power distribution systems [71], reverse power flow [72], power loss reduction [73], and voltage regulation [74].

Finally, the joint scheduling and operation of GfG and PtG units within an integrated system can attain a steady return on investment when operated for both electricity and gas price arbitrage exploitation, renewable energy surplus absorption, and providing ancillary services to the grid, i.e., optimal mix.

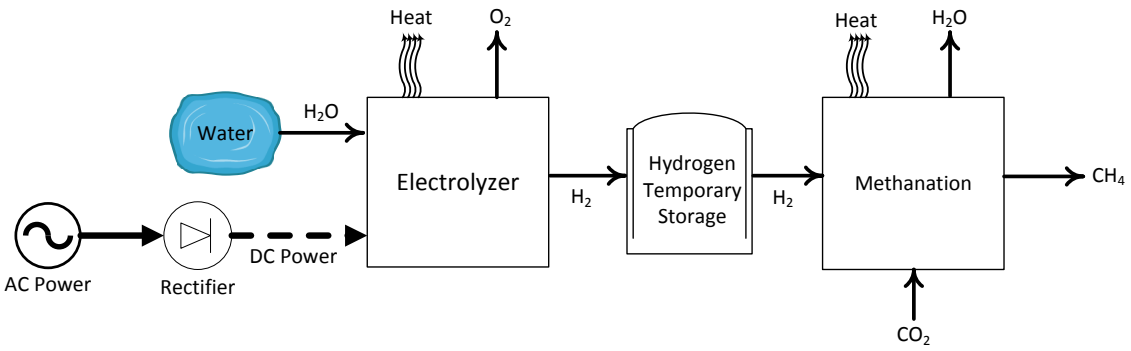


Figure 2.3: The steps of power-to-gas process.

2.2.2 Power–to–Gas Technology

The term PtG in the literature refers to the production of hydrogen or methane depending on the process involved and the use of the final product. The first step in PtG technology, illustrated in Figure 2.3, is the production of hydrogen gas from water. This step is known as *electrolysis* process in which electricity is used to split water molecules into hydrogen and oxygen. The produced hydrogen can then be either stored as is or used as input into *methanation* process to produce a Synthetic Natural Gas (SNG), methane, that is injected into the natural gas grid and stored for later use or transmitted to a different area [68].

The operating principle of the electrolyzer is illustrated in the chemical reactions presented in equation (2.1) that is induced by applying direct current (DC) power to decompose pure water molecules [75]:

$$2H_2O(liquid) \rightarrow 2H_2(gas) + O_2(gas) \tag{2.1}$$

The exact dynamic of the reactions in equation (2.1) depends on the type of electrolyzer technology. There exist three types of technologies: Alkaline Electrolyzer (AEL), Polymer Electrolyte Membrane (PEM) electrolyzers and Solid Oxide Electrolysis Cell (SOEC). Table 2.1 summarizes the main technical differences between those three electrolyzer technologies [76].

Table 2.1: Comparison between electrolyzer technologies

Characteristics	**AEL**	**PEM**	**SOEC**
Cell temperature (°C)	60–90	50–80	700–900
Load flexibility (% of nominal load)	20–100	0–100	-100/+100
Cold start-up time	1–2 h	5–10 min	hours
Warm start-up time	1–5 min	<10 s	15 min
Nominal system efficiency (LHV)	51–60%	46–60%	76–81%
Specific energy consumption (kWh/Nm^3)	5.0–5.9	5.0–6.5	3.7–3.9
Max. nominal power per stack (MW)	6	2	<0.01
Cell area (m^2)	<3.6	<0.13	<0.06
Investment costs ($/kW)	950–1750	1650–2500	(>2400)

The natural gas transported in the pipeline system is a mixture of hydrocarbon gases consisting primarily of methane. Other gases are also commonly found in the natural gas mixture such as alkanes, carbon dioxide, nitrogen, hydrogen sulfide, or helium. Injecting excessive amounts of hydrogen gas into the natural gas system is restricted due to several issues associated with the mix of gases that are permitted to be transported in the natural gas pipelines. Some of those challenges are:

- Hydrogen gas has a lower energy density compared with other gases in the natural gas mix, hence blending extra amounts of hydrogen will reduce the thermal energy capacity.

- Hydrogen embrittlement, also known as hydrogen-assisted cracking, causes the em-

brittling of metal pipelines after being exposed to hydrogen. Embrittled pipes can further develop cracks over time.

- The size of the hydrogen molecule is very small compared to the methane which increases the leakage rate of the hydrogen. It was highlighted in [77] that large leakage of hydrogen may cause economic and safety concerns.

- Burning hydrogen on the consumer side can be harmful to the gas appliances designed to run on methane, such as burners, boilers, or gas engines.

The methanation process involves converting hydrogen and CO_2 to methane as described in the following overall chemical equation:

$$CO_2(gas) + 4H_2(gas) \rightarrow CH_4(gas) + 2H_2O \tag{2.2}$$

The reaction in equation (2.2) can occur in two ways: catalytic or biological, depending on whether a chemical catalyst or biological micro-organisms are used to facilitate the conversion from hydrogen and CO_2 to methane with the former being more suitable in large industrial plants [78]. The efficiency of the methanation process varies between 72.7% without heat recovery and may reach up to 89.2% when heat recovery is used [78].

Finally, PtG technology has been in operation in many plants worldwide. For instance, a plant in the town of Markham, Ontario, Canada houses a 2.5 MW PEM electrolyzer that is being operated by the province's Independent Electrical System Operator (IESO) for balancing short–term real-time power supply and demand imbalances [79]. Another 20 MW project has been constructed in Quebec and began hydrogen production operation in late 2020 [80]. Many worldwide projects have been set up as well, such as 1 MW and 6 MW PtG plants, in Denmark and Germany, respectively [81] to absorb the excess wind power. An additional list of PtG projects can be found in [82].

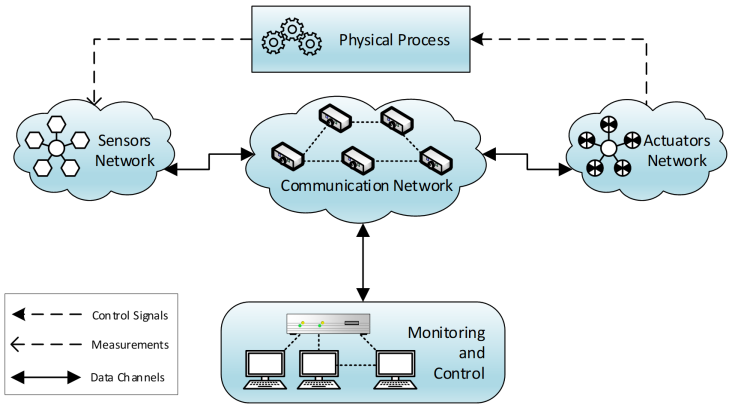


Figure 2.4: Typical CPS structure

2.3 Cyber Physical Systems Security Challenges and Countermeasures

A cyber–physical system is a closed-loop system of networked sensors and actuators, where data collected by sensors are communicated to embedded systems (controllers) that adjust the system's operation through the actuators. The typical structure of a CPS is shown in Figure 2.4. Modern SGss are forms of CPS due to the integration of ICTs into the various components of the power grid [83]. Therefore, being a form of CPS means that all the types of the different cyber–physical attacks are relevant to the SG structure.

Attacks that target CPSs can be classified according to their location into four main groups as shown in Figure 2.5. The attacker may launch coordinated attacks that combine multiple methods [84]. Accordingly, in the figure under the "*cyber*" category, the attacks are delivered through the cyber layer of the targeted system. Command manipulation represents a change in the commands that are already stored in the system without creating new commands while in code manipulation the adversary changes the software or the firmware of the system according to their adversarial objectives. In malware injection attacks, a virus or a worm is injected into the system and hijacks other running applications. The attacks under FDIAs manipulate the system's data without affecting the code of the system. Other cyber-based attacks include password cracking, supply chain

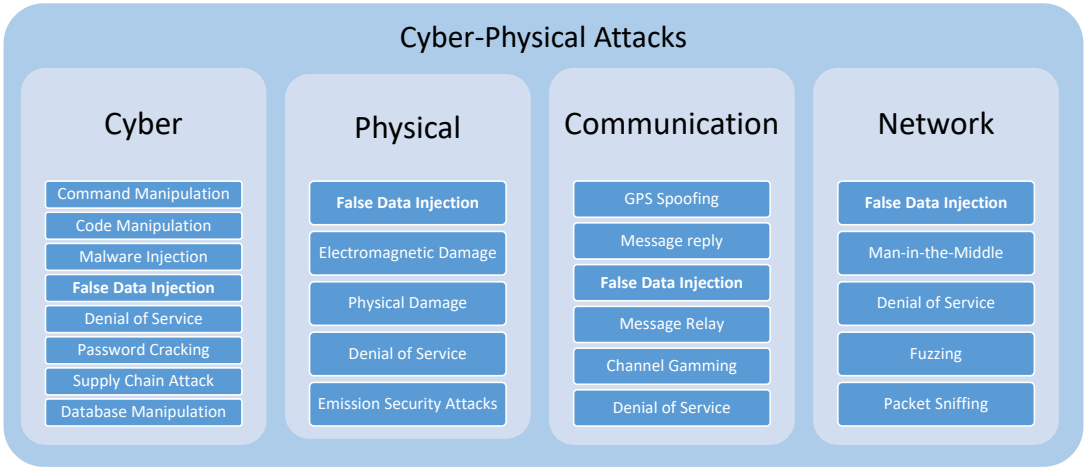


Figure 2.5: Type of attacks targeting CPSs based on the location of the attack.

attack, Denial of Service (DoS) attack, and database manipulation [85]. On the other hand, the "*physical*" attacks happen when the adversary performs some sort of physical interaction with the system such as causing damage by direct touches. Alternatively, without physically touching the physical parts, it is possible to damage the system by sending Electromagnetic pulses or injecting signals at overvoltage levels.

In the "*network*" attacks category, the adversary utilizes virtual network access to construct the attack without impacting the software or the firmware of the system or the physical communication link. The main type of attack under this category is the DoS where the network becomes inaccessible due to a large volume of malicious packets. FDIAs that are performed in the network layer where the attacker manipulates the data within the packets in the network. Other types include man-in-the-middle, packet sniffing, and fuzzing. Attackers usually perform spy-based attacks like packet sniffing as a preparatory step for FDIA. It is worthy to mention that DoS attacks causing disruptions in the legitimate user connectivity are clustered under network layer attacks whereas the attacks that disrupt the legitimate user services fall under Application layer attacks [86].

Similar to physical attacks, attacks under the "*communication*" category are done in the actual physical communication link without influence on the virtual network of

the CPS. These attacks could be developed either by breaking down the communication channel (channel jamming) or by delivering falsified messages (FDIA). GPS spoofing is a form of FDIA on the GPS signal delivered to the system where the adversary imitates the GPS signal and injects falsified data into it. Other attacks include message replay and relay. Communication attacks have a profound impact on the CPS since tremendous data is carried through these communication channels.

The research in [10] classifies the attacks into two types: *control-based* and *measurement-based*. Attackers with the right information can take advantage of control system flaws directly to affect the CPS in a direct and meaningful way. The effects of control-based attacks in SGs can range from transitory voltage and frequency instability, steady-state line overloading, and load shedding, to significant blackouts brought on by cascading failures, depending on the target systems or policy. Another serious risk to the SG is measurement-based attacks. Attackers can compromise measurements instead of directly manipulating control signals to impair situation awareness by hiding the incidence of disruptions or deceive control actions by reporting fictitious contingencies.

The *cost of the attacker* and the *cost of the defense* are two sorts of considerations that are frequently taken into account when designing an attack scheme. For the attacker, the resources and expertise needed to carry out the attack are often included in the costs; in many situations, the chance of the attack being discovered is also included. While for defense costs, the expenses often come from financial losses, equipment damage, and power interruptions.

Historically, several attack events have been reported on small to large-scale CPSs affecting all sectors such as energy, water, gas, finance, military, health, transport, and others. However, attacks on the energy sector have been the most high-profile. In the literature, the attack and defense strategies of CPSs are diverse and can mainly be grouped into theoretical, application, and defensive studies [87]. Firstly, under theoretical studies, researchers discuss the ability of the attacker to construct successful attack vectors. For instance, in [88], a simple approach is developed to determine the attack vector that can

increase the operation cost of the system. Next, application-wise research on FDIAs is focused on the impacts on the system operation or economics. For instance, the authors in [89] propose a method for exploring the cyber security of power grids. The physical response of power systems to malicious cyber–attacks is simulated to evaluate the risks associated with the cyber security issues. The authors in [90] propose a model to derive correlation indices based on attack goals that could be used to estimate attack consequences and identify critical parts of the system during coordinated attacks.

Proposing defense strategies is the main focus of FDIAs' defensive research work. Under this category, versatile detection methods have been proposed. For example, in [91], a cyber–constrained power flow model for enhancement of the smart grid resilience is presented. The authors take into consideration the impact of cyber networks on power grids and vice versa. In [92], the authors present a signature-based power system measurement source identification and authentication algorithm. The power system measurement signals are decomposed to extract the intrinsic components that are used for source authentication in the system. A method is presented in [93] that would mislead the grid attackers into designing ineffective attacks that cannot pass the SE module and control-related verification methods. The authors in [94] discuss the vulnerability of power grids that are subject to physical attacks in a situation where power systems and communication networks are interdependent. Such interdependence is due to the utilization of transmission line towers to set up the communication network utilized to control the power grid. In [95], a defense strategy in reaction to destabilizing cyber–physical attacks against power systems is presented. The presented model decouples the dynamics of a selected subsystem from the one that is affected by the attack. The authors in [96] propose a distributed blockchain-based framework to enhance the defensive capability of modern power grids against cyber–attacks. The authors argue that blockchain technology could be utilized to enhance the security of power systems via collecting data from the meters as nodes in a distributed network.

Lastly, several machine-learning-based techniques have been adopted for constructing

and detecting attacks against industrial control systems [97–100]. A Support Vector Machine (SVM)-based approach is proposed in [101] for the detection of stealthy attacks using supervised and unsupervised learning methods. In [97], the authors train a conditional Deep Belief Network (DBN) to extract patterns of normal system measurements and identify the changes in patterns during the attack. Nevertheless, an assumption is made that some of the system measurements are secure and the attacker is only able to compromise a subset of measurements. Another work in [98] proposes utilizing an unsupervised DBN-based network to model the system's normal behavior and detect any changes due to attacks. The authors in [99] propose machine learning-based attacks employing the SVM methods to construct undetectable attacks. However, their model requires injecting two types of agents: one for carrying on the attack while the other is to hide the false state of the Proportional-Integral-Derivative (PID)-controlled industrial plant. The work in [100] focuses on attacks against AC state estimation in power systems, presenting a detection method using the Recurrent Neural Network (RNN) model. However, none of the previous works have focused on investigating the cyber–physical security of IPGSs considering the attacks against the input/output signals in power and gas integration facilities.

2.3.1 False Data Injection Attacks

As part of the variety of cyber–physical attacks, FDIAs type represents a main category that has been extensively investigated for its range of types and impacts. Among these attacks, the threat of cyber–physical attacks can greatly affect the development and utilization of advanced power technologies. This section introduces FDIAs and sheds light on the significance of their impacts on CPSs. The survey in [10] highlights three major objectives in the existing FDIA schemes:

- *Least-effort attacks:* Find the sparsest attack vector with the least number of measurements to be compromised.

- *Least-information attacks:* Find the attack vector with the least required information on system topology.
- *Target-specific attacks:* Find the attack vector toward a specific post-attack effect.

In addressing this threat, several detection algorithms have been developed in the past few years. These were either model-based or data-driven approaches. Recently, several research works highlighted the vulnerability of traditional DC state estimators to FDIAs in which an adversary can introduce manipulated measurements to mislead system operators [17]. The attack will bypass traditional Bad Data Detection (BDD) in state estimation because the measurement residuals with false data injection attacks are the same as the measurement residuals with no false data injection attacks.

In FDIAs, the attacker aims to mislead the system's state estimation mechanism by sending corrupted measurements that will successfully pass the BDDs module and cause a wrong estimation of one or more of the state variables. Selecting the appropriate set of measurements to exploit among the accessible meters is most challenging and known to be an $L_0 - norm$ optimization problem.

AC state estimators were perceived immune against FDIA until the authors in [23] showed that although attacks targeting DC state estimators may not pass BDD in an AC state estimation, an adversary is still capable of injecting false data into the AC state estimation therefore both AC and DC state estimation approaches are vulnerable to the FDIA. In [24], nonlinear FDIA with inaccurate information was presented. Authors in [19] showed that an attacker can do an FDIA on a subnetwork without full information of the entire power network.

As an attacker, the problem of finding the attack vector is in general classified as an NP-hard [102]. In this regard, researchers have proposed several attack vector construction methods considering centralized and decentralized models. The authors in [102] proposed a greedy method to search for a subset of measurement to be protected by Phasor Measurement Units (PMUs). In [103], the authors constructed a relationship between attack detectability and network observability using a graph-theoretic model. Machine

learning tools have been proposed in [101] to detect stealth attacks in state estimation. In [104], a hierarchical architecture has been proposed to construct sparse attack vectors using combinatorial search methods. Mitigation schemes of FDIAs on state estimation have been analyzed in [105]. An attack detection approach using an artificial neural network was presented in [106]. An evolutionary approach based on a genetic algorithm for state estimation has been proposed in [107]. More reviews on the attack vector construction and state estimation methods in power systems have been presented in [25, 87, 108].

2.3.2 IoT-Devices Security in Power Systems Applications

The number of Internet of Things (IoT) devices being deployed over the past decade has been drastically increasing and is expected to approach 28 billion devices in 2025 [109]. A large portion of which that controls smart home and ambient computing devices are independently installed by consumers to provide convenient means to monitor and control their appliances (e.g., air conditioners, heating systems, lighting systems, smart plugs, electric vehicle chargers, etc), improve power utilization efficiency and enhance their level of comfort [110]. Illustrated in Figure 2.6 is a typical 3-layer IoT structure where layer-1 includes devices equipped with sensors, and/or actuators, and communication modules. In layer-2, a series of communication gateways and cloud channels are utilized to transmit collected information and receive commands from remote data storage, analysis, and modeling units in layer-3. This structure allows heterogeneous IoT devices to communicate with each other [111]. For instance, an IoT-based smart home management system collects information about the consumer's daily appliance utilization routines and sends it to an external service that models their behavior. Using the learned routines and other external factors such as electricity prices, the smart home system schedules the appliances to operate at preferred levels such as setting the temperature preference of an IoT-enabled air conditioner based on the preferred thermostat settings and weather forecast retrieved from an external cloud server.

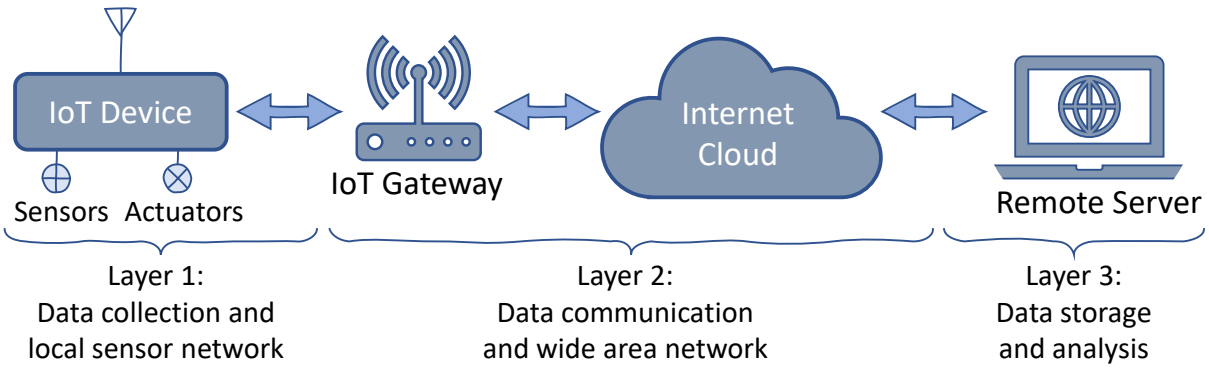


Figure 2.6: The structure of a typical IoT-enabled device communication with the cloud-based services.

2.3.3 IoT Vulnerability

Due to their interconnectedness and relatively weaker security measures, IoT devices are subject to cyber–attacks by adversaries exploiting known zero-day vulnerabilities [112]. IoT manufacturers tend to overlook cyber-security issues to reduce costs and maintain the rapid development cycle competitive with others [113]. Therefore, IoT devices are often designed with limited computational and storage capabilities hindering their ability to implement resilient defense mechanisms [114]. Additionally, many of these devices are installed and controlled by consumers with elementary security knowledge. Many researchers have reported security issues in a type of IoT-based voice-activated personal assistant devices, e.g. Alexa Echo and Google Home, that can lead to stealing sensitive information and launching man-in-the-middle attacks [115–117]. Ultimately, besides threats to the smart home's internal comfort and operation, compromised IoT-enabled devices to pose a threat to the external power distribution grid [118].

Adversaries can design attacks to target less secure elements such as IoT devices. The objectives of the attackers can also be different when attacking IoT devices compared to utility-scale attacks. That is, adversaries may seek personal profit rather than causing damage to the system. For example, attacks targeting electricity market infrastructures, such as tampering with sensor measurements or price signals sent by the utilities, can give

advantages to some agents over others [34]. Although there are no reported incidents of large-scale attacks on IoT-enabled appliances, similar attacks have been reported in the IT industry. As such, over 600,000 IoT devices have been infected with Mirai malware [119]. The malware exploited default factory settings for credential authentication and accessed a large network of IoT devices to form a network of bots (botnet). The compromised devices within the botnet, without consumers' awareness, were utilized to launch hours-lasting massive cyber–attacks on an internet service provider causing interruption to the online operation of many IT companies [120].

IoT technology has been applied in smart buildings, healthcare systems, agriculture, smart cities, and smart homes, among other application domains [10, 121–123]. Recently, many households are adopting the new trend of appliances that are individually equipped with IoT technologies or under a unified Smart Home Energy Management System (SHEMS) [124]. Efforts have been focused on identifying and designing control schemes for appliances with higher electrical consumption [125]. Among these common loads, are washing machines, Heating, Ventilating and Air Conditioning (HVAC) units, dishwashers, freezers, and Electric Vehicle (EV) chargers. IoT-enabled appliances utilize networked sensing and actuation, cloud computing, and artificial intelligence to make smarter decisions, which also make them naturally more vulnerable to threats in cyberspace. While the majority of these threats are not entirely new, the implications they leave in the CPSs generate subsequent threats to the physical systems being controlled and the safety of the occupants.

Many research works studied the security of SHEMSs in the efforts to secure SGs [126]. In addition, researchers have also considered the privacy issues related to revealing customers' information intensifying the threats to SHEMSs [127]. The research work in [128] divides IoT into three layers and analyzes the security requirements of each layer. Under this framework, SHEMS security falls under the application layer highlighting that application-specific security issues need to be analyzed for individual applications differently from the other layers. In [129], a taxonomy of the cyber–physical threats to

Figure 2.7: Types of the physical impact of cyber–physical attacks on SHEMSs.

SHEMS is presented under which the physical impacts are grouped into five high-level impacts, shown in Figure 2.7, triggered without the user's approval. The researchers in [130] were able to compromise both commercial and industrial IoT smart energy meters proving that security vulnerabilities are real for IoT devices. The work in [131] studies the cyber–attacks that target the pricing signal sent to the smart meters of the community to mislead the smart controllers to increase the peak energy load. The authors highlight that attackers can design an attack to invoke a particular response from smart loads that will impact a larger area power grid. The research in [132] proposes a machine-learning method for securing smart meters by detecting anomalies in cyber events and linking them with abnormal meter readings. However, the vulnerability of IoT-enabled appliances was not studied.

Research works in [20, 133, 134], studied the vulnerability of power distribution systems to FDIAs that target the smart meters in the network. All of them assume the attacker has gained access to the meter readings transmitted to that state estimation in the SCADA center. However, none of the previous works considers attacks that impact the demand in the network.

Chapter 3

Two-fold Intelligent Approach for Successful FDI Attack on Power Systems State Estimation

The objective of this research work, published in [135], is to propose a new intelligent approach to construct an optimal False Data Injection Attack (FDIA) vector against nonlinear State Estimation (SE) schemes. The search for optimality is based on an evolutionary Genetic Algorithm (GA), which is a type of metaheuristic search. Optimality of the attack vector is defined in terms of minimizing both its norm and the error it will cause to the Bad Data Detection (BDD) module. Once the components of the attack vector are identified, a neural network model is trained to model the optimal attack vector to generate real-time component values that can be utilized by an attacker to launch real-time attacks. Accordingly, FDIAs performed using vectors constructed via the proposed approach will require fewer resources to compromise and have a high success rate. Identifying optimal attack vectors helps in understanding the weaknesses in the SE of the power system. By understanding these weaknesses, resiliency approaches can be proposed to secure the system.

3.1 Introduction

In the literature survey presented in Section 2.3.1, the susceptibility of state estimators in power systems to FDIA has been discussed. These attacks can be very costly for the power system as they can cause blackouts, and can even be used as part of a denial-of-service attack. Even so, for an adversary, constructing an optimal attack vector - known as the least effort attacks - is a difficult task that requires solving a non-convex optimization problem in real-time using limited computational resources. In addition, this requires the attacker to access a high number of the system's measurements in real-time which is infeasible due to the limited resources the attacker possesses. Alternatively, the adversary may consider utilizing linearized models of the system to improve the speed of finding the optimal attack. However, this will result in inaccurate attack vectors that are easy to detect by the BDD module. Therefore, this chapter proposes an intelligent approach to optimally construct the FDIA vector using two-fold.

In the first fold, the problem of selecting the vector components is formulated as a constrained nonlinear programming optimization problem which is solved using a GA approach. In the second fold, an Artificial Neural Network (ANN) is trained to generate in real-time the vector amplitudes using data gathered from the compromised measurements. The optimality of the vector is measured in terms of three criteria: i) minimize the number of measurements required to be compromised, ii) consider the set of constraints on the measurements accessible by the adversary, and iii) maximize the flexibility of the vector to successfully pass BDD mechanism of the state estimator during various network loading conditions. Next, a case study is conducted to assess the performance of the proposed approach in generating optimal attack vectors to compromise the states of an IEEE 14-bus system. In the study, two different attack strategies have been considered in the system while varying the loading conditions.

The chapter ends with a discussion of the findings and a summary of the major outcomes of the study, which reveals that it is possible to craft effective attacks with only a few compromised power flow measurements. Thereby, securing those measurements will

strengthen the security and resiliency of the system against FDIAs.

3.2 Problem Formulation and Preliminaries

3.2.1 Nonlinear and Linear State Estimation Models

The SE process in power systems is to infer non-directly measured quantities that constitute the system state from other directly measured quantities known as system measurements. Considering the power system shown in Figure 3.1, we denote the set of system buses as Ω where $d = |\Omega|$ is the number of buses ($d = 14$ in this example). Let $\mathbf{z} \in \mathbb{R}^{m\times 1}$ be a vector of m measurements and $\mathbf{x} \in \mathbb{R}^{n\times 1}$ be the vector of system state. The general nonlinear SE model, which retains the nonlinearity between measurements and system states, is formulated as:

$$\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{e} \tag{3.1}$$

where $\mathbf{e} \in \mathbb{R}^{m\times 1}$ is the vector of measurement errors in which we assume that the error associated with each measurement i follows a normal distribution with zero mean ($\mu_i = 0$) and variance σ_i^2. We also assume that measurements are mutually independent so the error covariance matrix $\mathbf{R}$ is only diagonal.

In nonlinear SE, a common measurement set includes active and reactive power injections P_k and Q_k at bus k, and active and reactive power flows $P_{k,s}$ and $Q_{k,s}$ on the transmission line between buses k and s. In practice, not all those measurements are taken but a subset that renders the system observable, i.e. all system variables can be estimated. On the other hand, system state variables are voltage magnitude V_k and phase angles δ_k at each bus k of system buses except the angle of the slack bus which is set as reference zero.

The function $\mathbf{h}(.)$ is a nonlinear function, which can be decomposed into:

$$\mathbf{h}(\mathbf{x}) = [\mathbf{h_1}(\mathbf{x}), \mathbf{h_2}(\mathbf{x}), \ldots, \mathbf{h_m}(\mathbf{x})]^T \tag{3.2}$$

where $\mathbf{h_i}(\mathbf{x}) = h_i(x_1, x_2, \ldots, x_n)$ is a nonlinear function relating particular measurement

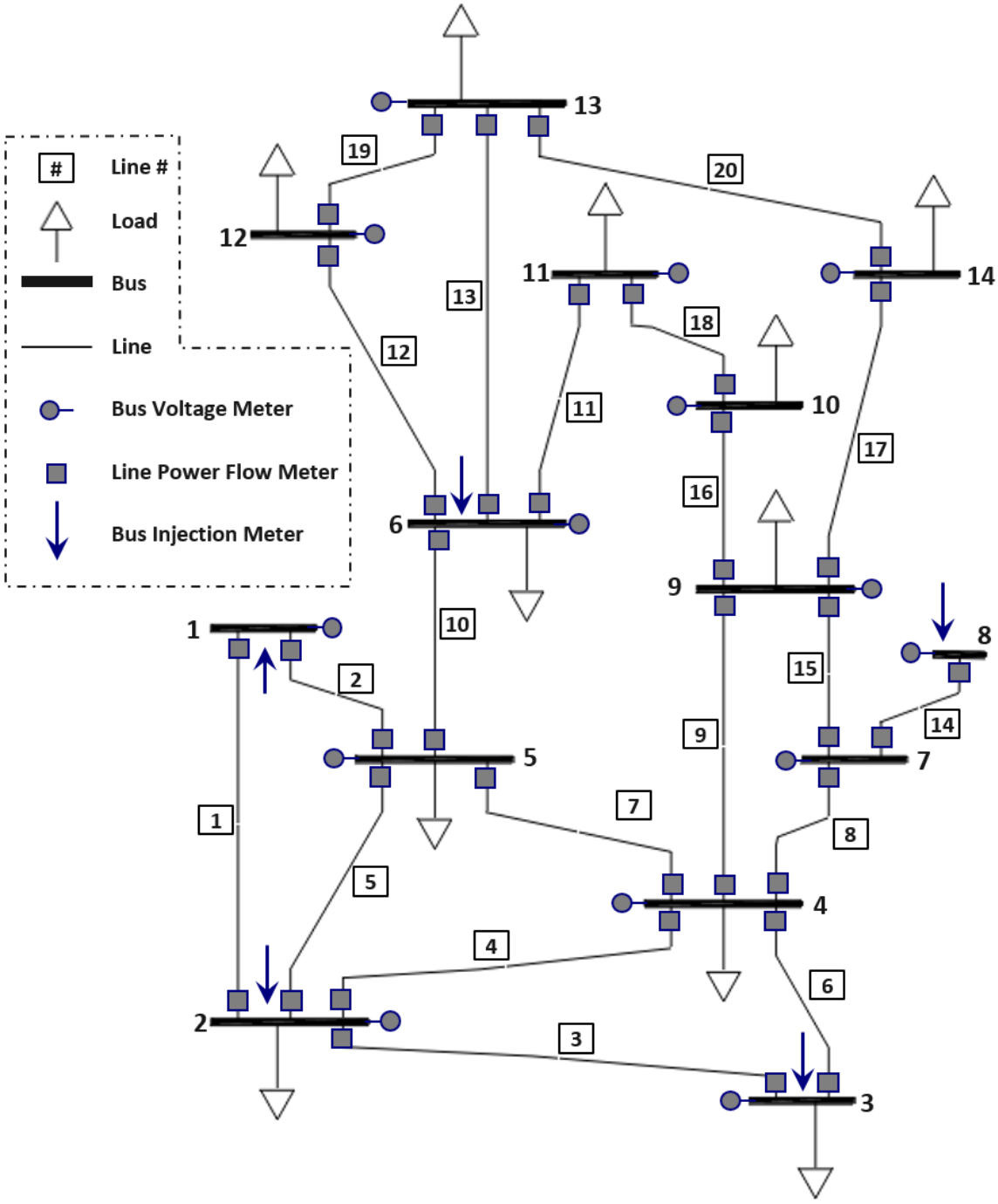


Figure 3.1: Placement of metering units on the IEEE-14 Bus System.

z_i with the state vector $\mathbf{x}$. The actual form of this function depends mainly on system parameters. For instance, the functions relating the measured real and reactive power injection at bus k and the real and reactive power flow from bus k to bus s are given in (3.3), (3.4), (3.5), and (3.6), respectively.

$$P_k = \quad V_k^2 \sum_{s\in\Omega_k} g_{ks} - V_k \sum_{s\in\Omega_k} V_s \left(g_{ks} cos\theta_{ks} + b_{ks} sin\theta_{ks}\right) \tag{3.3}$$

$$Q_k = -V_k^2 \sum_{s\in\Omega_k} b_{ks} + V_k \sum_{s\in\Omega_k} V_s \left(-g_{ks} sin\theta_{ks} + b_{ks} cos\theta_{ks}\right) \tag{3.4}$$

$$P_{k,s} = \quad V_k^2 (g_{sk} + g_{ks}) - V_k V_s \left(g_{ks} cos\theta_{ks} + b_{ks} sin\theta_{ks}\right) \tag{3.5}$$

$$Q_{k,s} = -V_k^2 (b_{sk} + b_{ks}) - V_k V_s \left(g_{ks} sin\theta_{ks} - b_{ks} cos\theta_{ks}\right) \tag{3.6}$$

where Ω_k is the set of buses that have transmission lines connected to bus k. While $\theta_{ks} = \delta_k - \delta_s$ denotes the voltage phase angle difference between buses k and s. Finally, g_{ks} and b_{ks} are respectively the conductance and susceptance of the line between buses k and s.

The solution ($\hat{\mathbf{x}}$) to the SE model in (3.1) is commonly obtained by solving the following Weighted Least Square (WLS) optimization problem in (3.7) where iterative methods such as Gauss-Newton are usually implemented [136].

$$\min \;\; J(\mathbf{x}) = [\mathbf{z} - \mathbf{h}(\mathbf{x})]^T \mathbf{R}^{-1} [\mathbf{z} - \mathbf{h}(\mathbf{x})] \tag{3.7}$$

Solving the optimization problem in (3.7) iteratively is known to be computationally intensive hence a linearized SE model is proposed as follows:

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e} \tag{3.8}$$

where $\mathbf{H}$ is a constant $m \times n$ Jacobian matrix determined by physical grid connections and line characteristics. The vectors $\mathbf{z}$, $\mathbf{x}$, and $\mathbf{e}$ have the same meaning and definition as those in the nonlinear SE model.

The weighted least squares method still can be applied to find the estimated system state ($\hat{\mathbf{x}}$) of the linearized SE model by optimizing:

$$\min \;\; J(\mathbf{x}) = [\mathbf{z} - \mathbf{H}\mathbf{x}]^T \mathbf{R}^{-1} [\mathbf{z} - \mathbf{H}\mathbf{x}] \tag{3.9}$$

Fortunately, this optimization problem has a closed-form solution given by:

$$\hat{\mathbf{x}} = \left(\mathbf{H}^T\mathbf{R}^{-1}\mathbf{H}\right)^{-1}\mathbf{H}^T\mathbf{R}^{-1}\mathbf{z} \tag{3.10}$$

3.2.2 Bad Data Detection (BDD) Approach

BDD techniques are utilized to detect measurement errors arising from either (i) meters inaccuracy issues, (ii) unintentional communication channel interference, or (iii) intentional interference by an adversary. Once bad data are detected, they need to be identified and eliminated or corrected, to obtain an unbiased state estimate.

Traditional BDD mechanisms are based on measurements residual analysis such as the largest normalized residual [136], given in (3.11).

$$\mathbf{r} = \mathbf{z} - \mathbf{h}(\hat{\mathbf{x}}) \tag{3.11}$$

Assuming *errors* in the measurements are mutually independent and follow a normal distribution, the residual magnitude squared $\|\mathbf{r}\|^2$ follows the Chi-squares (χ^2) distribution. Hence, the values of this residual error are compared to a threshold value τ based on a certain confidence level to detect the existence of bad data [136].

3.2.3 False Data Injection Attacks

The way BDD checks for errors allows carefully crafted erroneous measurements to pass to the SE in what is so-called False Data Injection Attacks [17]. In [24], it was shown that from the actual measurement vector $\mathbf{z}$, the adversary with knowledge of the system topology and state can replace $\mathbf{z}$ with a compromised vector $\mathbf{z}_a = \mathbf{z} + a$ which will pass the BDD test if:

$$a = \mathbf{h}(\hat{\mathbf{x}} + \mathbf{c}) - \mathbf{h}(\hat{\mathbf{x}}) \tag{3.12}$$

where $\mathbf{c}$ is a vector corresponding to the incurred change in the estimated state variables due to the attack. This shows that as long as the adversary can maintain the measurement residual less than the BDD threshold τ, the system will not detect the attack.

3.2.4 Optimal Attack Vectors Formulation

A rational adversary with an objective to perform FDIA would carefully select an attack vector, with a minimum number of measurements to compromise, that does not trigger a residual test. This can be formulated in the following optimization problem:

$$\begin{aligned} \text{minimize} \quad & \|a\|_0 \\ \text{s.t.} \quad & \|\mathbf{r}\| < \tau \end{aligned} \tag{3.13}$$

where $\| \cdot \|_0$ is the L_0-*norm* of the vector.

Several optimization techniques to solve (3.13) have been proposed assuming linear SE models [137], however, few researchers tackled this issue considering nonlinear SE models. Limitations of linearized approaches for attack vector construction include the use of a fixed Jacobian system matrix $\mathbf{H}$ and ignoring the internal system state. Hence, many of the attacks constructed using linearized SE will fail when applied on nonlinear state estimators [23]. Certainly, constructing attacks that pass linear and nonlinear SE will be advantageous to the adversary.

3.3 Proposed Two-fold Attack Vector Construction Approach

To solve the optimization problem in (3.13), a GA is proposed that utilizes a nonlinear state estimator in the fitness function. As shown in Figure 3.2, in the first step the attacker would gather all the relevant information about the system topology and parameters to build a simulation model of the targeted system. In the next step, the attacker determines the targeted system state to manipulate in the attack. This target state can be one of the system's state variables or one of the measured values.

The following step is to run GA to find a set of attack vectors with the least number of measurements. In this step, the attacker can reduce the measurement search space by removing inaccessible ones or those difficult to compromise. Afterward, the vectors are

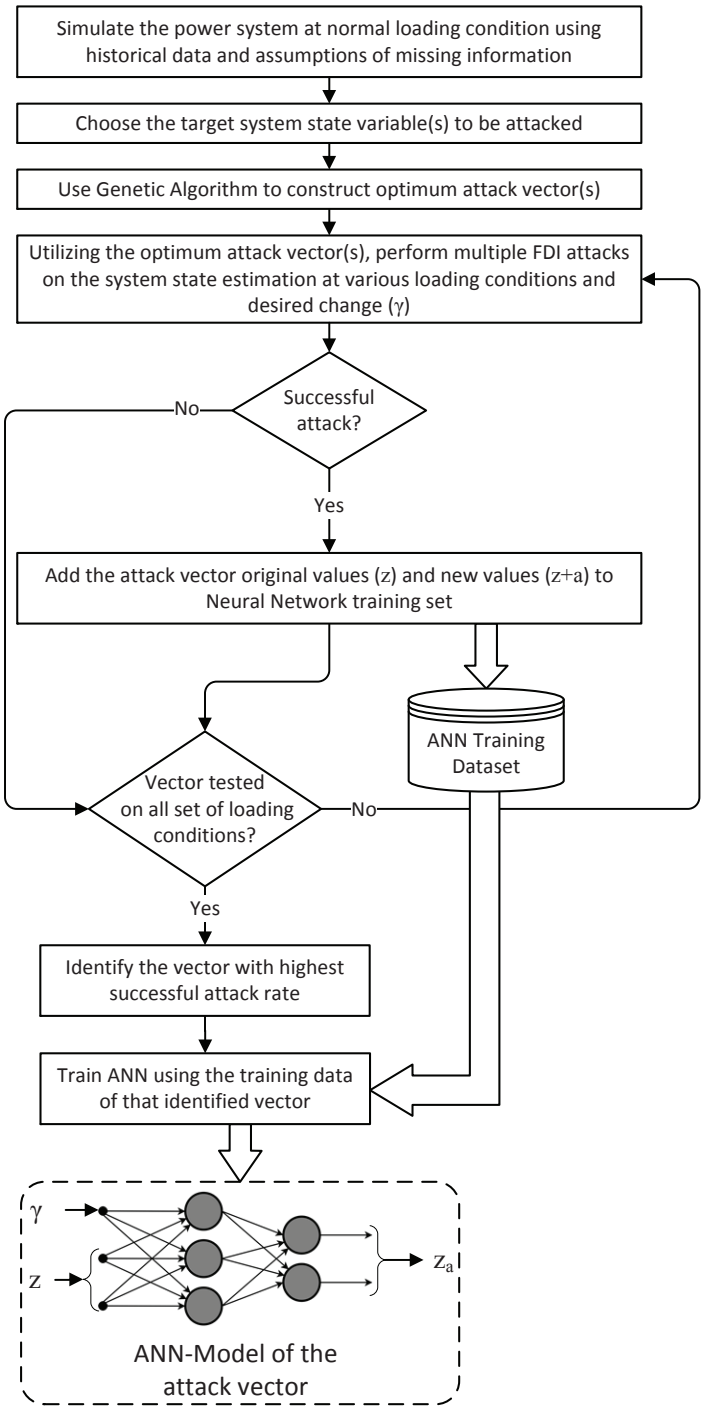


Figure 3.2: Flowchart of the proposed two-fold method to construct optimal attack vectors.

ranked based on their flexibility to construct a successful attack during various loading conditions and desired deviation in the targeted system variable (see Section 3.4.3 for more details). Finally, an ANN model will be developed for the top-ranking vector(s) that will generate instant values of the attack vector components with a high probability of a successful attack.

3.3.1 Step1: Identification of Vector Candidates

GAs are popular heuristic optimization techniques that are utilized to search for optimal solutions in highly nonlinear and high dimensions problems. Starting with an initial set of solutions, called population, each solution is analogous to a chromosome in biological genetics. Solutions are assessed using a fitness function that ranks all the solutions in a particular population. Generally, a certain fraction of chromosomes with high fitness value are retained in the current generation while the rest are discarded. To make up the population number, the maintained chromosomes are replicated then crossovers and mutations are applied to the chromosomes. This process is repeated for a given number of iterations until the chromosomes eventually converge to an optimum. Compared to the other heuristic techniques, GAs, with proper tuning of their parameters, are less susceptible to being stuck in local minima.

In the proposed implementation, binary value chromosomes are adopted representing the existence of a certain measurement in the attack vector. Chromosomes that form an attack vector that cannot be adjusted to pass the BDD algorithm in SE will be given a low fitness value. On the other hand, the ones which pass BDD will be assigned a fitness value inversely proportional to the number of measurements and the amount of measurement residual r. More details of the GA implementation are provided in Algorithm 1. After running the GA algorithm several times the set of optimum attack vectors is identified. Then, the optimal vector is selected and modeled via a neural network.

Algorithm 1 Minimal critical measurement set

Require: a, av – the state variable to be attacked and the targeted value, respectively.

function GETMINATTACKVECTOR(a,av)
  $z \leftarrow Actual\ Measurements$
  $x \leftarrow h^{-1}(z)$
  Initialize Genetic Algorithm (GA)
  while (GA did not converge) **do**
    for all $p \in$ GA Population **do** ▷ $p \in \{0,1\}^m$
      $z^* \leftarrow z$
      repeat
        $z' \leftarrow z^*$
        $z'(a) \leftarrow av$
        $x' \leftarrow h^{-1}(z')$
        $z' \leftarrow h(x') + e$
        $z^*(p) \leftarrow z'(p)$
        $E \leftarrow sum(\|x - x'\|^2)$
      until $E < \tau$
    end for
  end while
  return $argmin_{p \in \text{GA Population}}(|p|)$
end function

3.3.2 Step2: Modeling Attack Vectors Using ANN

ANN is a computational structure that comprises interconnected groups of artificial neurons that mimic biological brains. In ANNs, each neuron is associated with an input value vector (x^i) and a set of weights (w^i). Sets of neurons are grouped together forming the layers of the ANN. Usually, ANNs have an input layer, the first layer, and an output layer which is the final layer. In the middle, there should be at least one hidden layer. Among the various architectures of ANNs have been developed, Multilayer Perceptron (MLP) neural network is being the most effective model for function approximation.

Let $x = [x_1, x_2, \cdots, x_m]^T$ be the neural network input and $y(x) = [y_1, y_2, \cdots, y_n]^T$ be the output. Starting from random initial internal parameters w (weights), the neural network is trained by gradually adjusting those parameters so that the error between the

MLP output $\hat{y}(x, w)$ and the true output $y(x)$ is minimized:

$$min \left\| \hat{y}(x, w) - y(x) \right\|_2 \tag{3.14}$$

The training process is iteratively performed in two phases: forward propagation and weight update. During the first phase, the input value is propagated from the input layer, via the hidden layers to the output layer using the current weight value and offset value of the network then the output error of the network is computed. In the second phase, the weights are continuously updated and modified to minimize the error.

In the simulation, the MLP neural network model with two hidden layers in addition to the input and output layers is adopted. The size of the input is set by the number of measurements in the attack vector $\|z_a\|_0$ in addition to one extra parameter λ determines the amount of desired change in the targeted system state variable. The number of output variables matches the number of measurements in the attack vector.

3.4 Numerical Results

3.4.1 System Model

The IEEE 14-bus system shown in Figure 3.1 is utilized to test the effectiveness of the proposed algorithm. The measurements available to the SE module comprise the active $P_{k,s}$ and reactive $Q_{k,s}$ power flowing from bus k to bus s, and active P_k and reactive Q_k bus power injection at buses {1, 2, 3, 6, and 8}. The attack target is to manipulate the amount of active power flow in the system lines. All simulations were run in Matlab, using MATPOWER [138] package.

System Loading Conditions: A range of overall system loading between 135 MVA and 520 MVA was simulated. The active and reactive power distribution among the system buses was also varied.

Table 3.1: Optimal Attack Vectors Components Results: target state active power flow measurements in lines #12, #8 and #15

Target Measurement	**PF12**	**PF08**	**PF15**
Actual Value (p.u.)	0.0779	0.2807	0.2807
Target Value (p.u.)	0.1167	0.5615	0.5615
Optimal Attack Vector Size	4	3	3
	Vm12	**PF09**	**PF08**
Actual Value (p.u.)	1.0552	0.1608	0.2807
Attack Value (p.u.)	1.0509	0.1610	0.1351
	PF19	**PF15**	**QF08**
Actual Value (p.u.)	0.0161	0.2807	-0.0968
Attack Value (p.u.)	-0.0175	-0.2613	-0.1014
	QF19	**QF08**	**QF15**
Actual Value (p.u.)	0.0075	-0.0968	0.0578
Attack Value (p.u.)	0.0219	-0.0746	0.0671
	PG04		
Actual Value (p.u.)	0.0000		
Attack Value (p.u.)	0.0219		
Estimation Error	7.5×10^{-4}	9.5×10^{-4}	9.9×10^{-4}

** PF: Active Power Flow, QF: Reactive Power Flow, PG: Power Injection, Vm: Voltage Magnitude*

3.4.2 Attack Vector Variables Selection

After setting the target as manipulating the active power flow measurement in the lines, the GA is run several times to identify the set of optimal attack vector candidates. The vector with the lowest number of variables over all the runs was chosen as the attack vector to the corresponding targeted state variable (active power flow). The results presented in Table 3.1 show the list of measurements to compromise when targeting the power flow in line#12, line#8, and line#15. The table shows the actual value of the measurement

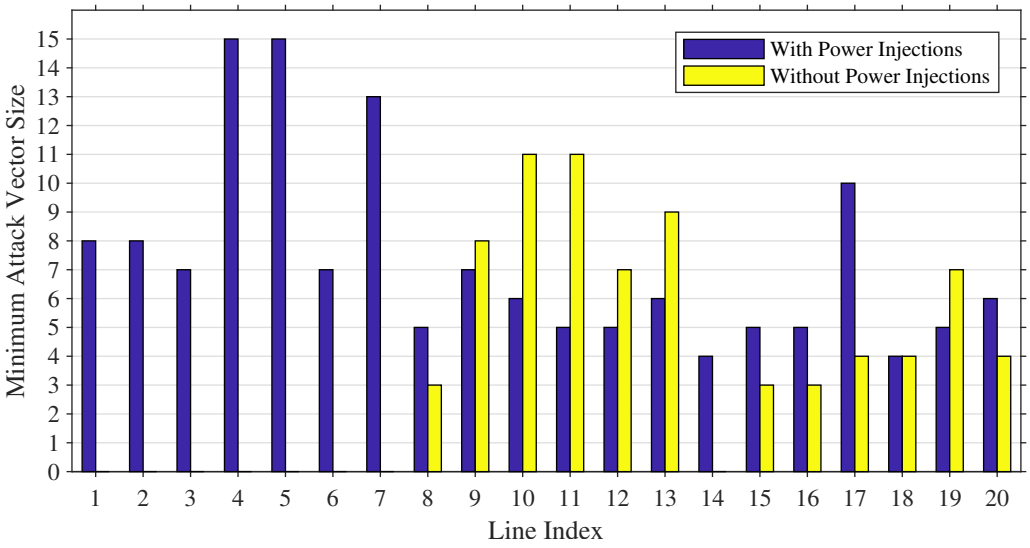


Figure 3.3: Minimum attack vector size to perform successful FDIA targeting lines' active power flow.

and the false value to be set by the adversary to bypass the BDD test and the estimation error.

With regards to the adversary's capabilities to access the measurements, two scenarios are considered: (1) The adversary can compromise active and reactive power injection measurement at system buses and active and reactive power flow in the lines. (2) The adversary can only compromise active and reactive power flow in the lines. The results are shown in Figure 3.3, where the bars represent the minimum optimal attack vector size (y-axis) which is the number of measurements to compromise in order to successfully attack the power flow of the line identified by the line index (the x-axis). The figure indicates that without corrupting power injections, attacks on power flow in lines #1 to #7 and #14 will not be successful. This is because those lines are connected to at least a bus with a generation unit and there is no easy way to compensate for power flow corruption via the other lines.

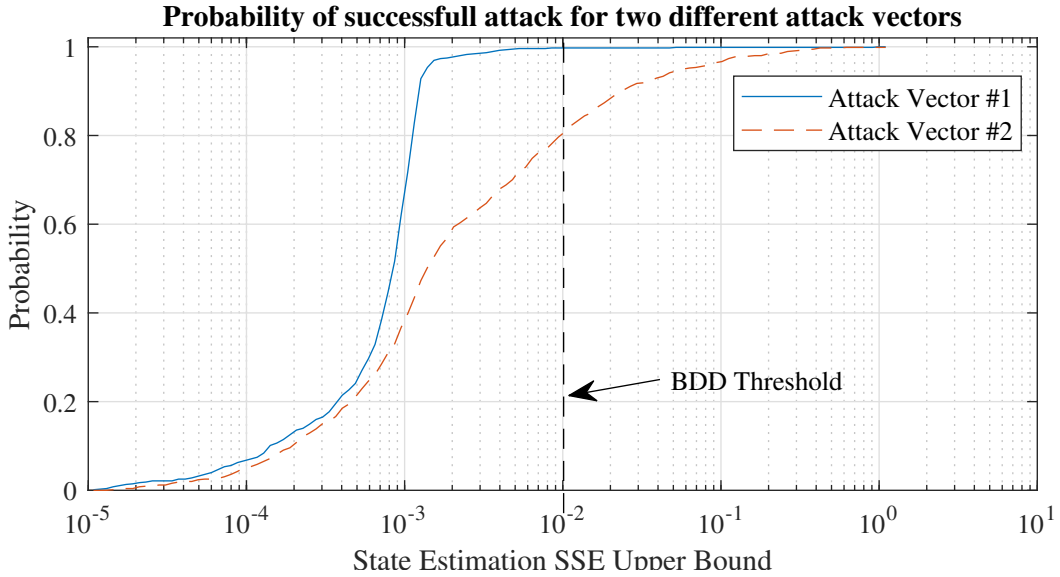


Figure 3.4: The rank of two attack vectors #1 and #2 according to their probability of performing successful FDIAs.

3.4.3 Attack vector Ranking

The optimization problem in (3.13) has different solutions which means there will be multiple attack vectors that can be used to target the same system state variable. Moreover, unlike linearized SE, in nonlinear SE an attack vector that can be used to construct a successful attack during certain system loading conditions may fail during other loading conditions (residual error being above BDD threshold τ). Therefore, an adversary will be interested in maximizing the vector utilization to cover a wide range of system loading conditions. Hence, we introduce the following metric to rank how a certain vector is performing at variable loading conditions:

Definition 1: (*SSE Upper Bound Probability* — SSE_{UB}) is the probability of getting the Sum of Squared Errors (SSE) in the SE less or equal to a specific error value τ when running an attack under variable system operating conditions and attack desired change

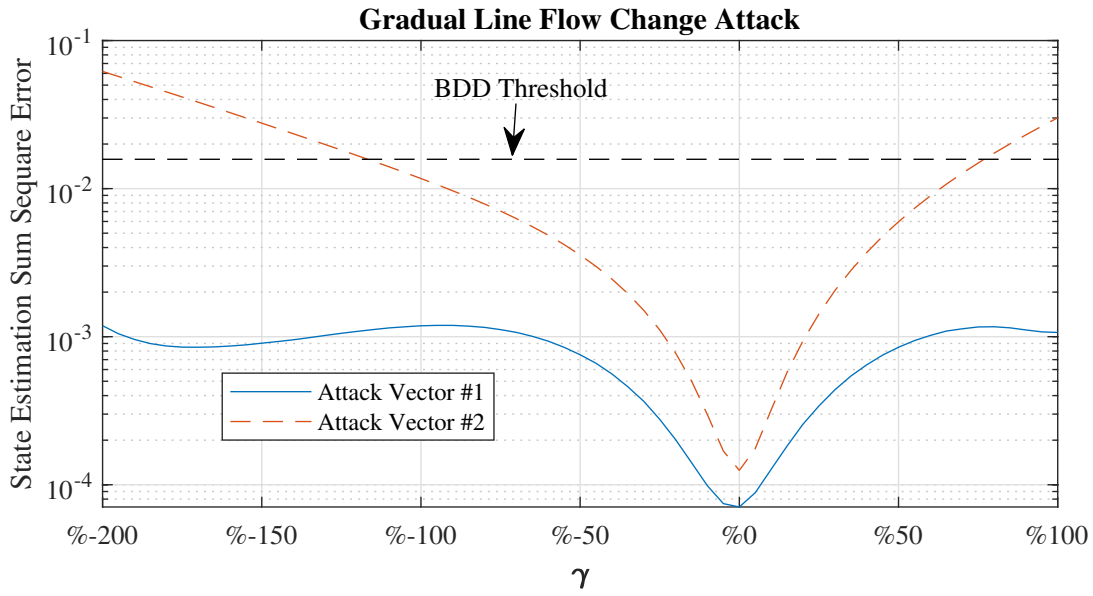


Figure 3.5: Average SSE under two ANN-modeled attack vectors #1 and #2 target gradual change in the line power flow.

severity.

$$SSE_{UB} = Pr(SSE \leq \tau) \tag{3.15}$$

Figure 3.4 shows the results at $\tau = 0.01$ for two different attack vectors that target corrupting active power flow in the line #12, i.e., $P_{6,12}$. In the first attack vector #1, ($SSE_{UB} \approx 1$) adversary can manipulate both lines' active power flow and bus power injections measurements, while in the second attack vector #2, ($SSE_{UB} = 0.8$) only line power flows can be manipulated. It can be seen that attack vector #1 is more efficient than #2. Moreover, the close to unity value of SSE_{UB} in attack vector #1 confirms that the ANN is effectively able to model this attack vector and generate successful attacks.

3.4.4 Ramp-up Attack Strategy

Gradual change attacks are performed by slowly changing the targeted state variable so state estimators equipped with historical information verification will not trigger BDD alarm. In this study, a gradual change attack is simulated by changing the targeted value

by γ ranging between %-200 and %100.

The results shown in Figure 3.5 demonstrate that attack vector #1 can construct successful attacks for all the desired change range while attack vector #2 fails when $\gamma < -\%90$ and $\gamma > \%60$. Details of the attack vectors and affected state variables are plotted in Figure 3.6.

3.5 Summary and Discussion

This chapter presents a novel two-fold intelligent approach to constructing successful FDIAs against any SE method. First, the optimal attack vector is selected using GA then an MLP neural network is trained to generate the values of the vector variables. This approach was tested on nonlinear SE and simulation results demonstrate its efficacy to produce successful attack vectors during variable system loading conditions and different attack target severity. It was also demonstrated that the use of MLP allows to efficiently model sophisticated attacks.

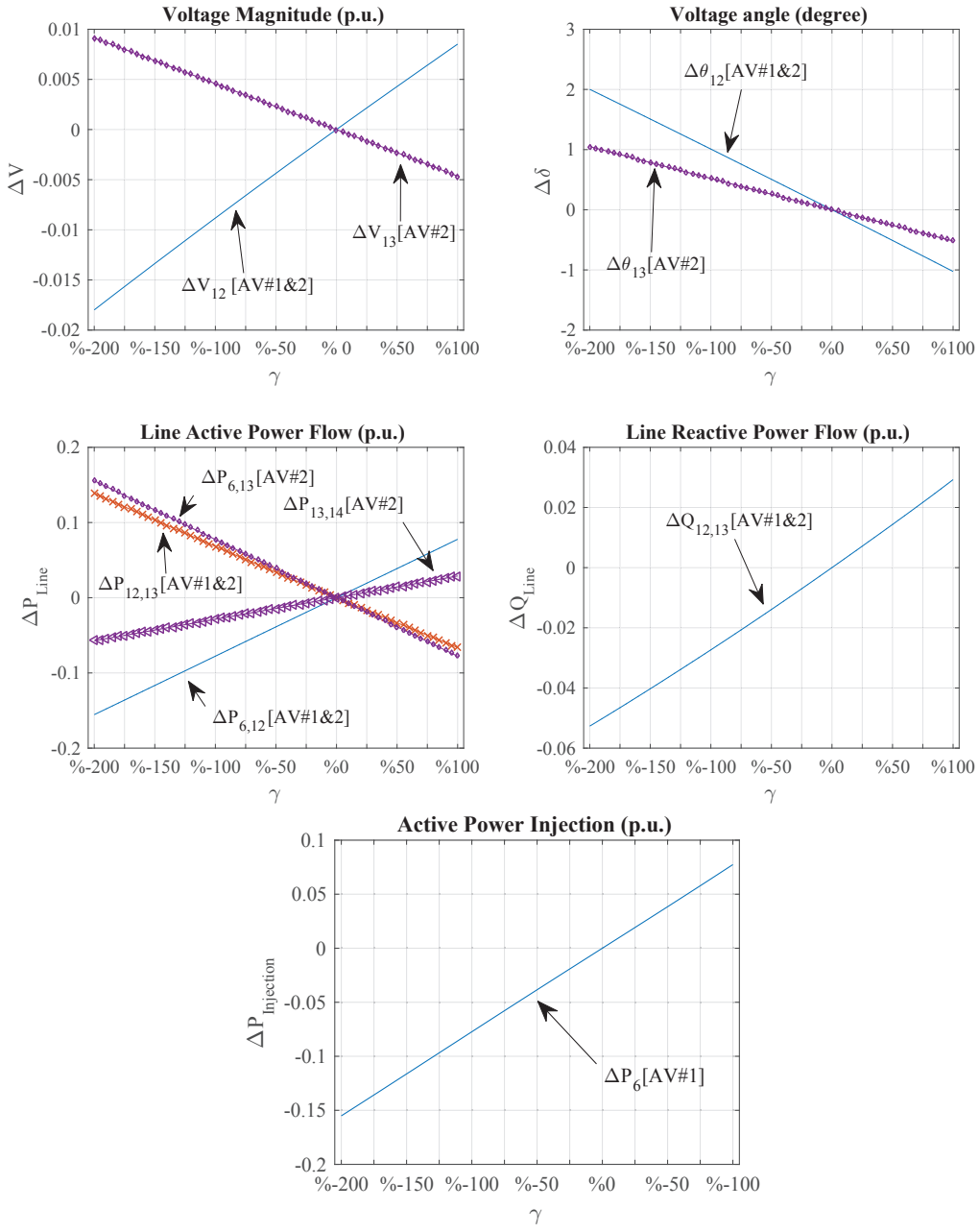


Figure 3.6: Comparing system state variables for two attack vectors #1 and #2 that target gradual change in the line power flow: (top-left) ΔV bus voltage change, (top-right) $\Delta\delta$ change in the bus angles, (middle-left) ΔP_{Line} change in the active lines power flow, (middle-right) ΔQ_{Line} change in the reactive lines power flow, and (bottom) $\Delta P_{injection}$ change in the buses power injection/generation.

Chapter 4

Framework for Evaluating Cyber–Attacks on Integrated Power and Gas Systems

4.1 Introduction

To investigate the resiliency of the Integrated Power and Gas System (IPGS) against cyber–attack, the operation scheduling models need to be established to simulate attack scenarios and evaluate their impacts on the physical layers of both power and gas systems. In this chapter, a new framework is presented which builds on the interdependency operation model of the power systems and gas distribution models using the steady-state models of both systems. Ultimately, the contribution of this chapter is to develop a framework with a set of modeling tools for cyber-security researchers to explore the vulnerability of the IPGS to cyber–physical attacks. Two research works are published in [139] and [140] confirming the validity of the proposed framework.

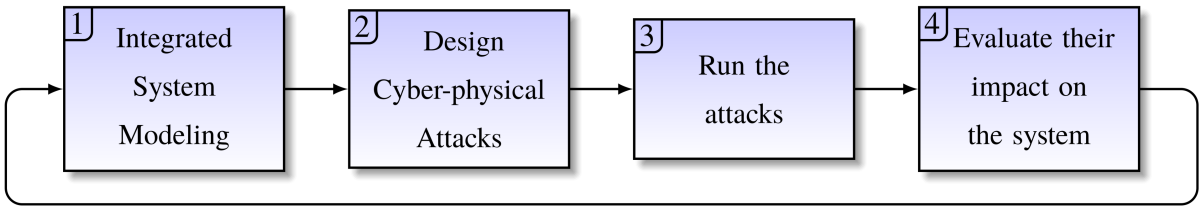


Figure 4.1: Framework steps for analyzing cyber–physical security of integrated power and gas systems

4.2 Framework Architecture

Figure 4.1 shows the framework steps. In step (1), the framework facilitates modeling the power and gas systems via providing a unified interface to model both systems and connect the integration resources. Step (2) allows designing a set of cyber–physical attack scenarios to be tested on the integrated system. In step (3), simulations are run for both normal and attack scenarios considering different system operating conditions. The last step (4), provides means for evaluating the impact of the attacks.

Considering the integrated system shown in Figure 4.2 which comprises a power transmission network with wind and Photovoltaic (PV) energy resources, a gas transmission grid, and Power–to–Gas (PtG) and Gas–fired Generation (GfG) units that integrate the two systems. The proposed mechanism of operation of the system is designed to operate the integrating facility in a way to maximize the arbitrage revenue while meeting the desired level of renewable energy penetration and maintaining the system operational constraints. This operation scheme is formulated by the following revenue maximization problem:

$$\text{Maximize}: \quad \sum_{t \in \mathbb{T}} \left(A^t - C^{t,\text{PtG}} - C^{t,\text{GfG}} - R^t \right) . \delta t, \tag{4.1}$$

where A^t is the total gas and power arbitrage revenue of PtG and GfG units generated by exploiting the energy market prices, $C^{t,\text{PtG}}$ and $C^{t,\text{GfG}}$ are the operation cost of PtG

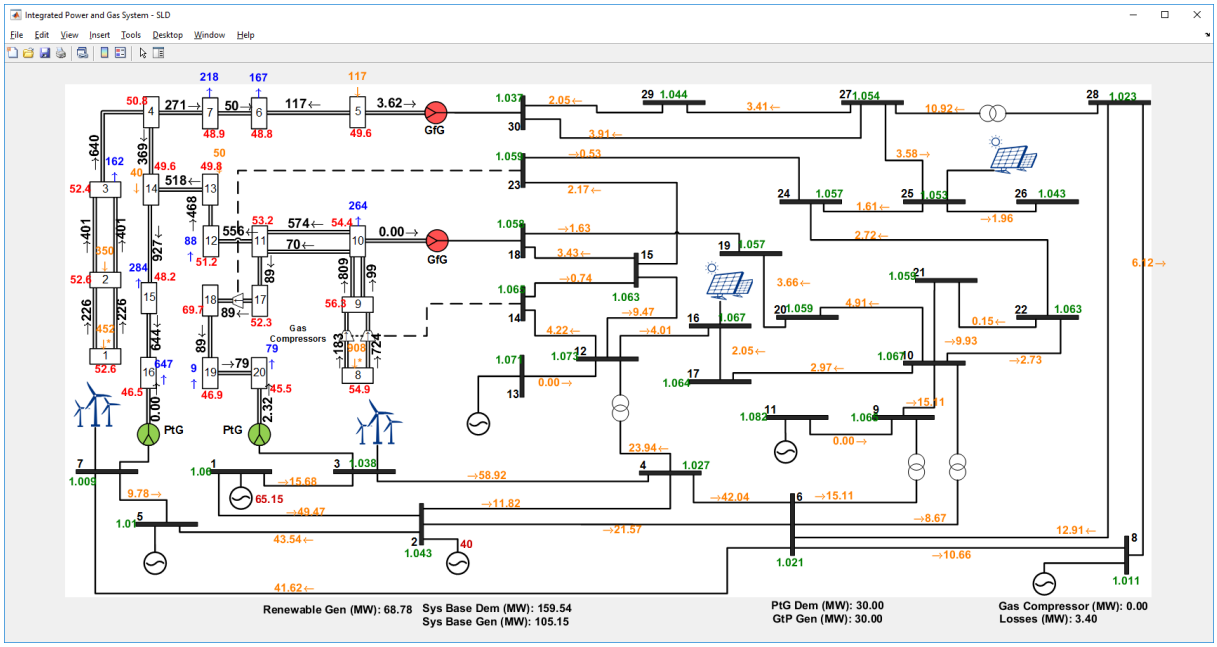


Figure 4.2: Screenshot of the main interface of the IPGS framework. The gas grid and nodes are shown on the top left along with the gas pressure, demand, and flow. On the right, the power system network is shown along with the power flow and voltages. The integration resources, PtG, and GfG units are shown in green and red symbols, respectively.

and GfG units, respectively, and R^t is the loss due to renewable energy penetration participation due to the operation of PtG units and ceasing the operation of GfG units. Particularly, this term is defined as:

$$R^t = \sum_{j \in \mathbb{N}} c_j^{\text{Ren}} . P_j^{t,CRen} \qquad \forall t \in \mathbb{T}, \tag{4.2}$$

where the variable $P_j^{t,CRen}$ represents the curtailed renewable energy of the resource at bus j; whereas the term c_j^{Ren} controls the curtailment of renewable energy, hence controlling the desired amount of renewable energy injected into the grid. As such, the higher this term is, the more renewable energy is penetrated.

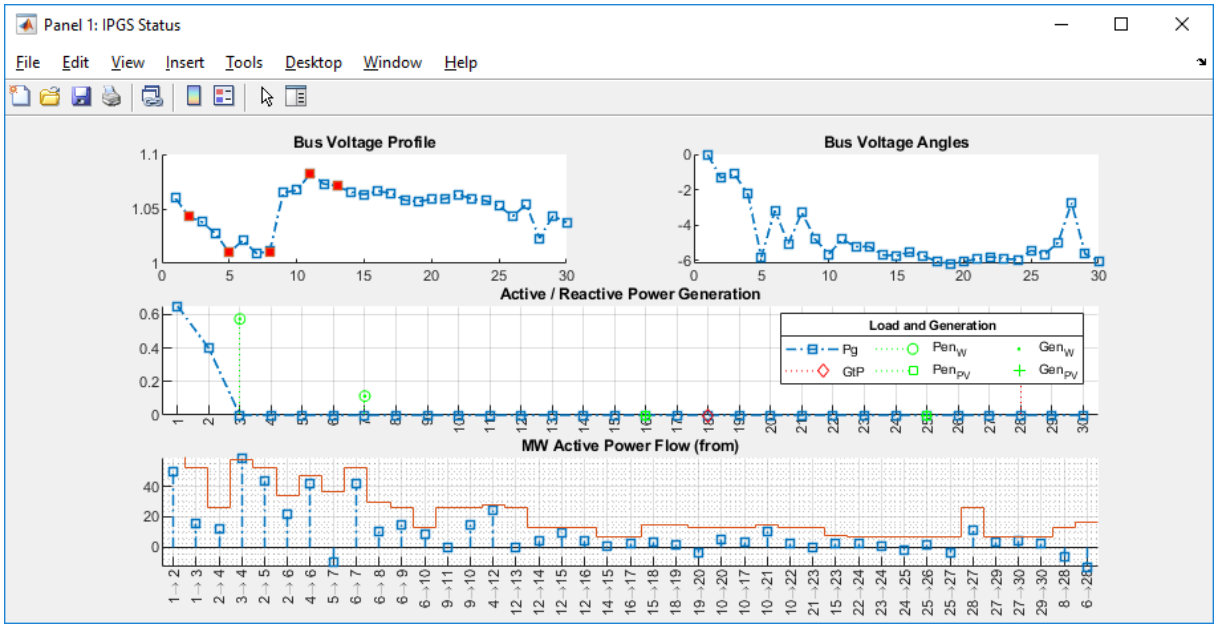


Figure 4.3: IPGS results panel showing the standard power system status signals. The bottom plot presents the power flow levels on power system lines along with lines' capacity shown in red.

4.3 Integrated System Model

Historically, the coupling of power and gas systems used to be unidirectional via GfG units, i.e., gas is burned to produce electricity. However, with the advancement of PtG technologies, both systems can be fully coupled to form an integrated system as depicted in Figure 2.2. To study the steady–state operation of the integrated system, both power and gas systems are modeled independently as conventional buses and lines in power systems, and nodes and pipelines in gas systems. Then, the coupling units are modeled considering energy conversion factors, as detailed in the following subsections.

4.3.1 Electrical Power System Model

Power systems are generally modeled as sets of buses $\mathbb{B}$, transmission lines $\mathbb{M}$, loads, and generators. The active P_j^{G} and reactive Q_j^{G} electric power, produced by a generator

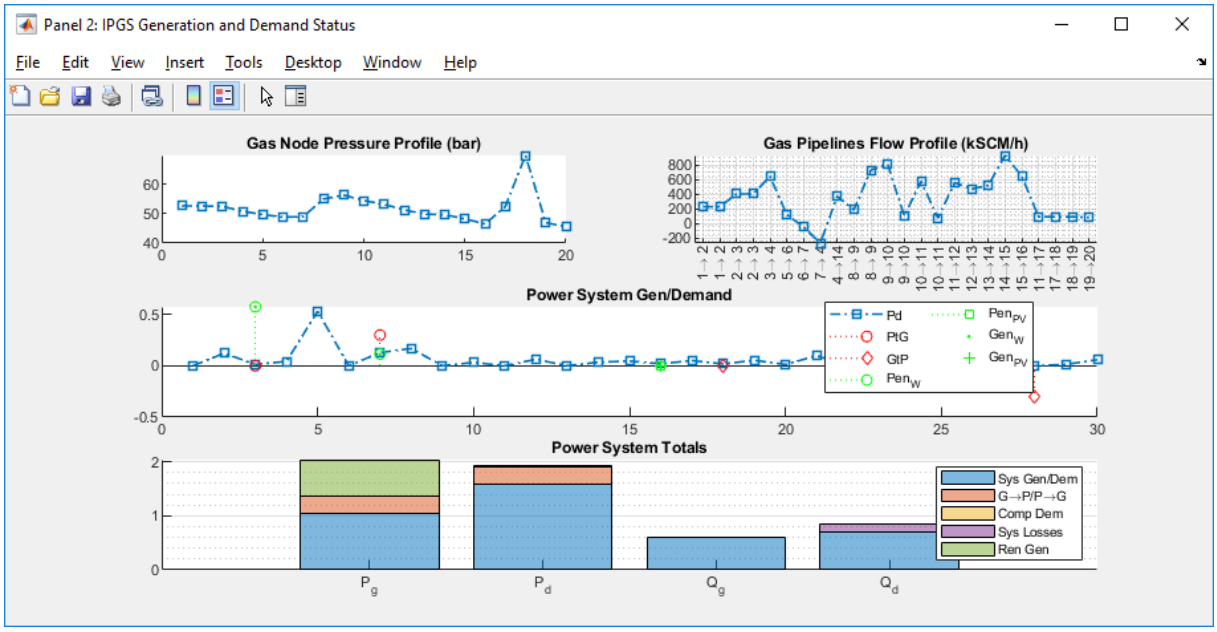


Figure 4.4: IPGS steady-state results panel showing gas pressure and flow profiles in the top two plots. The other plots show the power generation and demand levels, renewable power generation, PtG and GfG operation levels, and system losses.

located at bus $j \in \mathbb{B}$, flow on the transmission lines to feed the active P_j^{D} and reactive Q_j^{D} power demands of the loads connected to system buses. Given a particular loading and power generation state at a time t, the steady–state power flow study of the system reveals system buses' voltage magnitude $v_{t,j}$, and angle $\delta_{t,j}$ in the case of having a balanced system. As such, the power system can be formulated using the power balance equation given as:

$$P_{t,j}^{\mathrm{G}} - P_{t,j}^{\mathrm{D}} = v_{t,j} \sum_{k=1}^{N} v_{t,k} \left(\mathtt{G}_{jk} \cos \theta_{t,jk} + \mathtt{B}_{jk} \sin \theta_{t,jk} \right) \quad \forall t \in \mathbb{T} \wedge j \in \mathbb{B}, \tag{4.3}$$

$$Q_{t,j}^{\mathrm{G}} - Q_{t,j}^{\mathrm{D}} = v_{t,j} \sum_{k=1}^{N} v_{t,k} \left(\mathtt{G}_{jk} \sin \theta_{t,jk} - \mathtt{B}_{jk} \cos \theta_{t,jk} \right) \quad \forall t \in \mathbb{T} \wedge j \in \mathbb{B}, \tag{4.4}$$

where N is the number of buses; the constants $\mathtt{G}_{jk}$ and $\mathtt{B}_{jk}$ are, respectively, the conductance and susceptance of the line between the buses j and k; and $\theta_{jk} = \delta_j - \delta_k$ is the phase

angle difference between them. It is worth mentioning that $\mathbb{T}$ in the presented models represents the time horizon of the study.

4.3.2 Gas Flow in the Natural Gas System

Similar to power systems, gas systems are modeled as a set of nodes $\mathbb{N}$ interconnected with pipelines $\mathbb{L}$. That is, for a given gas node $l \in \mathbb{N}$, we denote the amount of gas demand as G_l^{D}, and gas source (wells) as G_l^{S}. Gas flow in the system is governed by the node's pressure Π_l, pipelines' hydraulic resistance coefficient $\mathtt{C}_{ll'}^2$, and pipeline type, i.e., passive or active pipeline (gas flow is enforced with a gas compressor). The steady–state analysis of the gas system reveals the gas pressure at the nodes and the flow rate $F_{ll'}$ inside the pipelines. Consequently, the following equations (4.5) and (4.6) model the gas flow in passive and active pipelines, respectively:

$$F_{t,ll'}.\,|F_{t,ll'}| = \mathtt{C}_{ll'}^2 \left(\Pi_{t,l}^2 - \Pi_{t,l'}^2\right) \quad \forall t \in \mathbb{T} \wedge \forall (l,l') \in \mathbb{L}_p, \tag{4.5}$$

$$F_{t,ll'}.\,|F_{t,ll'}| \geq \mathtt{C}_{ll'}^2 \left(\Pi_{t,l}^2 - \Pi_{t,l'}^2\right) \quad \forall t \in \mathbb{T} \wedge \forall (l,l') \in \mathbb{L}_a, \tag{4.6}$$

$$F_{t,ll'} \geq 0 \qquad\qquad \forall t \in \mathbb{T} \wedge \forall (l,l') \in \mathbb{L}_a, \tag{4.7}$$

where $\mathbb{L}_p$ and $\mathbb{L}_a$ are the set of passive and active pipelines, respectively. Equation (4.7) ensures that the gas flow direction in active pipelines is controlled by the associated gas compressor.

Eventually, the gas nodal balance is formulated in the following equation:

$$G_{t,l}^{\mathrm{S}} - G_{t,l}^{\mathrm{D}} = \sum_{l' \in \mathbb{N}_l} F_{t,ll'} \qquad\qquad \forall t \in \mathbb{T} \wedge \forall l \in \mathbb{N}, \tag{4.8}$$

where (4.8) states that at any gas node, the net total of the gas supply and demand shall be equal to the sum of outflow/inflow gas at that node.

4.3.3 Energy Conversion Between the Gas and Power Systems

This section presents the model for the three steady–state coupling parameters between the power and gas networks in the integrated system. Namely: (1) GfG units that burn

natural gas to produce electricity; (2) PtG units that consume electrical power in the process to produce gas; and (3) Gas compressors that are supplied with electric power from specific buses and run to control the pressures inside active pipelines in the gas grid.

Given the output electrical power P_j^{GfG} of a GfG installed at bus j, the amount of input gas needed G_j^{GfG} can be calculated using the following equation:

$$G_j^{\mathrm{GfG}} = \alpha^{\mathrm{GfG}} P_j^{\mathrm{GfG}} \tag{4.9}$$

where α^{GfG} represents the conversion factor of the GfG unit.

Similarly, the energy conversion relationship between the PtG gas generation G_j^{PtG} and the consumed power P_j^{PtG} is given as:

$$P_j^{\mathrm{PtG}} = \alpha^{\mathrm{PtG}} G_j^{\mathrm{PtG}} \tag{4.10}$$

where α^{PtG} denotes the energy conversion efficiency of PtG.

The electric power consumption P_l^{GC} of the gas compressor l can be calculated using the following equation [141].

$$P_l^{\mathrm{GC}} = \mathtt{K}^{\mathrm{GC}} \mathtt{Z}_a F_{\mathrm{C},l}^{\mathrm{gas}} \left[\frac{T_l}{E_c \eta_c}\right] \left[\frac{c_k}{c_k - 1}\right] \left[\left(\frac{\Pi_l^{\mathrm{out}}}{\Pi_l^{\mathrm{in}}}\right)^{\frac{c_k - 1}{c_k}} - 1\right] \tag{4.11}$$

where $F_{\mathrm{C},l}^{\mathrm{gas}}$ represents the natural gas flow in the compressor; Π_l^{in} and Π_l^{out} are pressures at suction and discharge flanges, respectively; T_i is the suction temperature in °R; $\mathtt{K}^{\mathrm{GC}}$ is unit conversion the factor; $\mathtt{Z}_a$ is the average compressibility factor; η_c is compression efficiency; E_c is compressors parasitic efficiency; c_k is specific heat ratio for natural gas.

4.3.4 Optimization Formulation

In this section, the formulation of an optimal scheduling algorithm is presented with the set of nonlinear constraints for the operation of the integrated system. It is assumed that there is no monetary incentive for the PtG–GfG facility to operate during low prices.

Facility Arbitrage Model

At time t, given the electricity price $\mathtt{E}_t^{\mathrm{P}}$ and the gas price $\mathtt{E}_t^{\mathrm{G}}$, the arbitrage revenue of the PtG–GfG units connected to the bus $j \in \mathbb{B}$ in the integrated system is formulated as follows:

$$A_{t,j}^{\mathrm{P}} = \left(P_{t,j}^{\mathrm{GfG}} - P_{t,j}^{\mathrm{PtG}}\right) . \mathtt{E}_t^{\mathrm{P}}, \tag{4.12}$$

$$A_{t,j}^{\mathrm{G}} = \left(G_{t,j}^{\mathrm{PtG}} - G_{t,j}^{\mathrm{GfG}}\right) . \mathtt{E}_t^{\mathrm{G}}, \tag{4.13}$$

$$A_t = \sum_{j \in \mathbb{B}} \left(A_{t,j}^{\mathrm{P}} + A_{t,j}^{\mathrm{G}}\right) \tag{4.14}$$

where equations (4.12) and (4.13) represent, respectively, the profit achieved by the power and gas purchase and sale using the PtG and GfG in the power and gas markets for the units installed at bus j. In (4.14) is the total arbitrage of all the units in the system at time t.

Operational and Capital Costs

The average hourly operational and capital costs combined for the facility are utilized and represented in \$/MWh with different values for each of the PtG and GfG units. Accordingly, let c_j^{PtG} and c_j^{GfG} denote the aggregated hourly cost of running PtG and GfG units located at bus j, respectively. The hourly operational and capital costs associated with each of the GfG and PtG facilities are formulated in (4.16) and (4.15), respectively:

$$C_t^{\mathrm{PtG}} = \sum_{j \in \mathbb{B}} c_j^{\mathrm{PtG}} . P_{t,j}^{\mathrm{PtG}} \qquad \forall t \in \mathbb{T}, \tag{4.15}$$

$$C_t^{\mathrm{GfG}} = \sum_{j \in \mathbb{B}} c_j^{\mathrm{GfG}} . P_{t,j}^{\mathrm{GfG}} \qquad \forall t \in \mathbb{T}. \tag{4.16}$$

The facility capital costs are set proportional to the units' size to match the size changes.

Renewable Penetration

PtG facility can help maintain the network balance by absorbing portions of surplus renewable energy instead of curtailing it. To model such behavior, an additional control

term is added to the objective function which forces PtG to operate despite the conditions for making arbitrage profit are not met. This term is given as follows:

$$R_t = \sum_{j \in \mathbb{B}} c_j^{\text{Ren}} . P_{t,j}^{\text{CRen}} \qquad \forall t \in \mathbb{T}, \tag{4.17}$$

where in (4.17), the term c_j^{Ren} penalizes the curtailment of renewable energy. As such, the higher this term is, the more renewable energy is absorbed.

4.3.5 Objective Function

The objective function of the optimization aims to maximize the arbitrage profit and renewable penetration, in addition to minimization of the operation cost terms. It is formulated as:

$$\text{Maximize}:$$
$$\sum_{t \in \mathbb{T}} \left(A_t - C_t^{\text{PtG}} - C_t^{\text{GfG}} - R_t \right) . \delta t, \tag{4.18}$$

Constraints

The objective function in (4.18) is subject to the following constraints:

- Operational constraints of the GfG and PtG units:

$$\underline{P_j^{\text{GfG}}} \leq P_{t,j}^{\text{GfG}} \leq \overline{P_j^{\text{GfG}}} \qquad \forall t \in \mathbb{T} \wedge \forall j \in \mathbb{B}, \tag{4.19}$$
$$\underline{P_j^{\text{PtG}}} \leq P_{t,j}^{\text{PtG}} \leq \overline{P_j^{\text{PtG}}} \qquad \forall t \in \mathbb{T} \wedge \forall j \in \mathbb{B}. \tag{4.20}$$

- Renewable energy penetration enforcement:

$$0 \leq P_{t,j}^{\text{CRen}} \leq P_{t,j}^{\text{Ren}} \qquad \forall t \in \mathbb{T} \wedge \forall j \in \mathbb{B}, \tag{4.21}$$

- Voltage and power flow constraints:

$$\underline{P_i^{\text{F}}} \leq P_{t,i}^{\text{F}} \leq \overline{P_i^{\text{F}}} \qquad \forall t \in \mathbb{T} \wedge \forall i \in \mathbb{M}, \tag{4.22}$$
$$\underline{Q_i^{\text{F}}} \leq Q_{t,i}^{\text{F}} \leq \overline{Q_i^{\text{F}}} \qquad \forall t \in \mathbb{T} \wedge \forall i \in \mathbb{M}, \tag{4.23}$$
$$\underline{v_j} \leq v_{t,j} \leq \overline{v_j} \qquad \forall t \in \mathbb{T} \wedge \forall j \in \mathbb{B}. \tag{4.24}$$

- The gas supply, demand, and nodal pressure constraints:

$$\underline{G_l^{\mathrm{S}}} \leq G_{t,l}^{\mathrm{S}} \leq \overline{G_l^{\mathrm{S}}} \qquad \forall t \in \mathbb{T} \wedge \forall l \in \mathbb{N}, \tag{4.25}$$

$$\underline{G_l^{\mathrm{D}}} \leq G_{t,l}^{\mathrm{D}} \leq \overline{G_l^{\mathrm{D}}} \qquad \forall t \in \mathbb{T} \wedge \forall l \in \mathbb{N}, \tag{4.26}$$

$$\underline{\Pi_l} \leq \Pi_{t,l} \leq \overline{\Pi_l} \qquad \forall t \in \mathbb{T} \wedge \forall l \in \mathbb{N}. \tag{4.27}$$

4.4 Case Studies

In Chapter 2, it was highlighted that connecting renewable energy resources can be problematic for the grid under large penetration. Renewable generation could be maximum during the periods when it is not needed or minimum when it is desperately required in the grid. The long–known conventional energy storage concept has been at the center of attention to deal with the intermittency of renewable generation [142, 143]. An alternative solution to the problem would be the conversion of surplus renewable power to Synthetic Natural Gas (SNG) using PtG units. Contrary to a conventional energy storage unit (e.g., battery storage), the energy can be displaced in an integrated gas and power grid; i.e., the surplus power is absorbed from one location in the power grid, converted to SNG, and injected into the gas grid. The gas, on the other hand, can be used to run a GfG unit to generate power at another location of the power grid when power is needed [144].

PtG and GfG facilities as private assets can be owned and managed by merchandise operators. Such facilities are contemplated as large–scale assets at the distribution level. Large–scale facilities can choose to deal with the Local Distribution Company (LDC) and trade the energy at Time–of–Use (ToU) rates; or can choose to trade with the wholesale electricity market and experience real-time pricing [145]. As private investors, PtG and GfG unit operators need to know which of the aforementioned scheduling approaches are more profitable; i.e., trading with LDCs at ToU rates or with the wholesale market at real-time prices.

Using the proposed framework, two case studies are conducted:

- **Case Study 1**: Investigates the optimal sizing of PtG units co–operated with existing GfG within an IPGS penetrated with renewable energy sources. The objectives of this study are to: (i) maximize the arbitrage revenue of the facility, and (ii) increase the renewable energy penetration while maintaining operation constraints in the integrated system.

- **Case Study 2**: Presents comparative ToU and wholesale price scheduling from the economic perspective to reveal the IPGS facility's profit under the two scheduling approaches. The individual and joint operation of the PtG and GfG units are investigated under both the ToU and wholesale electricity price scheduling. Numerical studies are conducted to evaluate the performance of the model on test systems using real-world operational data.

4.4.1 Case Study 1: Optimal Sizing of PtG Units toward Elevated Renewable Power Penetration

Few research works in the literature have investigated the optimal PtG unit sizing. For instance, in [81], a particle swarm optimization approach is presented to size PtG units in medium-voltage networks. The objective is to mitigate the impact produced by wind power on the stability of the distribution network and minimize system losses. The works in [146], the integrated system operation is formulated as a nonlinear optimization problem with the objective to minimize the operation and investment costs in the distribution system. However, none of the aforementioned studies considers the arbitrage revenue model of operation for the joint PtG–GfG facility.

Accordingly, the optimization objectives of this case study are to minimize the facility operating costs and maximize arbitrage profit, while increasing the penetration level of renewable energy. The facility operation is subject to the energy flow and a set of nonlinear constraint equations. The objective of optimal sizing is to maximize the overall utilization of the PtG units. The standard IEEE 30-bus system is utilized and real-world historical

data to illustrate the proposed approach. The results regarding utilization rate, renewable penetration rate, and revenue are discussed.

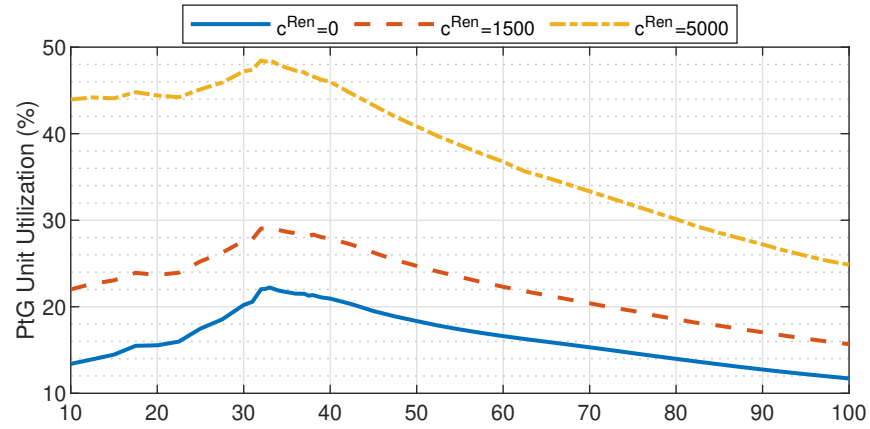
Simulated System

Simulations were run in Matlab on the IEEE 30-bus power system coupled with the Belgian natural gas system [147] through two PtG units connected at buses 3 and 7 and two GfG at buses 18 and 28. The schematic of the system has been depicted in Figure 2.2. A real-world load profile with a maximum and an average hourly load of 180 MW and 110 MW, respectively. The renewable power generation profile was generated from historical wind speed and solar irradiation data applied on resources rating at 200 MW wind and 40 MW PV. The average hourly power generated was 55 MW and 13 MW for wind and PV, respectively.

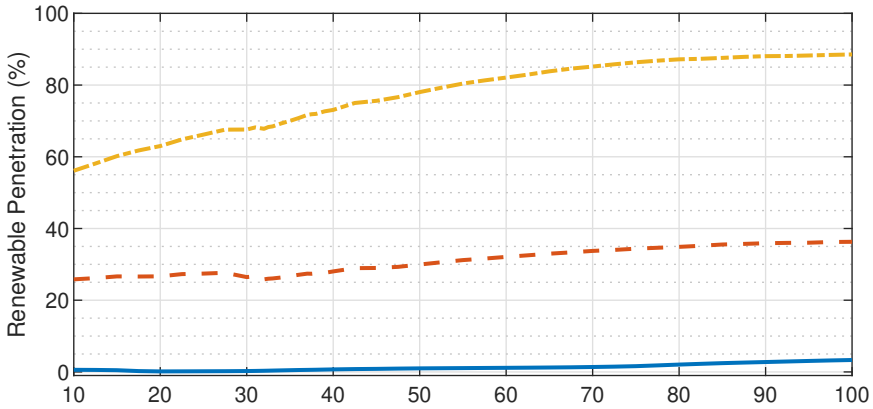
Results and Discussion

To find the optimal PtG unit size, the proposed optimal scheduling approach was run on hourly full-year data at variable ratings between 10 MW to 100 MW. Results of the utilization rate, renewable penetration, and revenue are shown in Figure 4.5 for three penalty c^{Ren} values (0, 1500, and 5000).

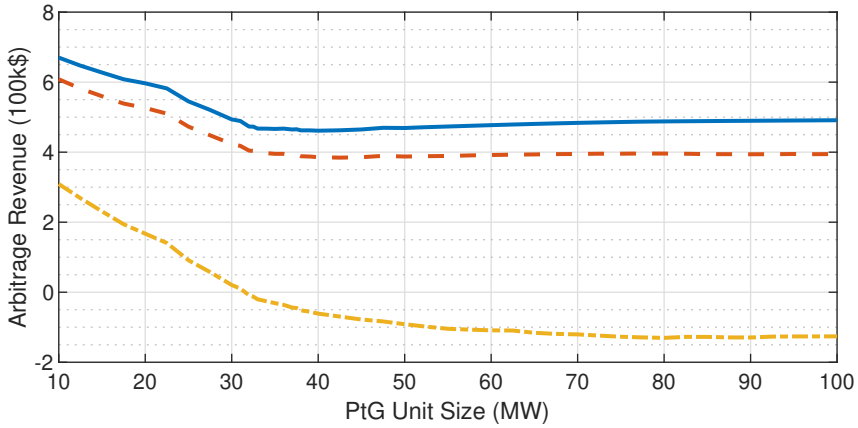
PtG Unit's utilization rate is defined as the normalized ratio of aggregated hourly PtG demand for a full year of operation over the rating. As shown in Figure 4.5a, PtG utilization reaches a global maximum peak when the unit size is around 32 MW. While small PtG sizes may allow the unit to run frequently at full capacity, the amount of yearly average operation is less than the PtG of the size 32 MW. Conversely, larger PtG sizes cause the PtG unit to operate less frequently at its full capacity, hence a lower utilization rate. Moreover, as anticipated in the optimization objective function, Figure 4.5a shows that the higher the enforcement parameter c^{Ren} value, the higher the utilization rate. Numerically, PtG utilization rates at the peaks are 22%, 30%, and 48% for the values of



(a) Average yearly PtG utilization (%)



(b) Renewable energy penetration (%)



(c) Arbitrage Revenue

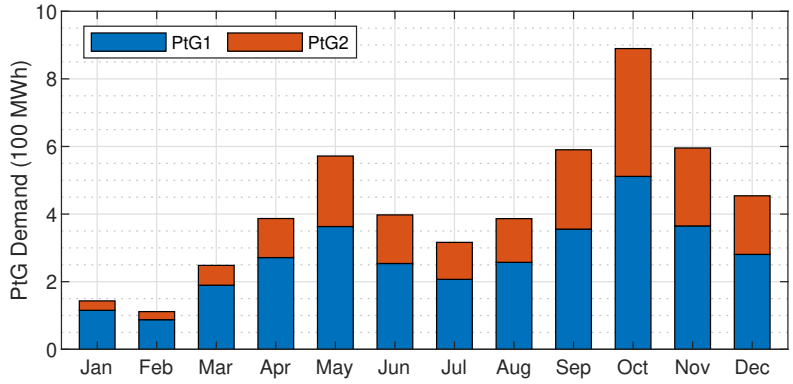
Figure 4.5: The impact of PtG unit size (MW) on (a) Average yearly utilization (%), (b) Renewable energy penetration (%), and (c) Arbitrage revenue of the facility.

c^{Ren} as 0, 1500, and 5000, respectively. This would, in turn, implies that PtG operation increases to absorb more renewables.

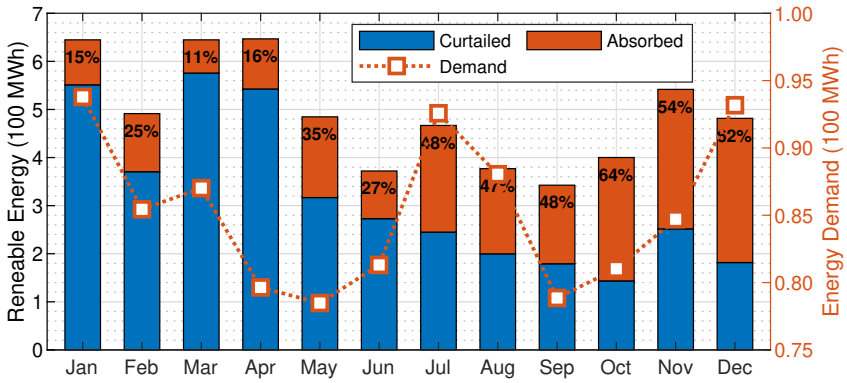
Figure 4.5b and Figure 4.5c show the percentage of renewable energy penetration and arbitrage revenue of the facility, respectively. There is a trade-off between the amount the PtG facility can absorb from surplus renewables and the revenue it makes when only the arbitrage model is adopted for the operation. Hence, a service agreement can be established with the Independent Electrical System Operator (IESO) to compensate the facility for balancing the demand-supply with renewables. Using a high penalty value of c^{Ren}, the facility was able to absorb around 70% of the available renewables.

Using the optimal PtG size of 32 MW, Figure 4.6 shows the monthly operation results of the facility. The monthly operation of both PtG units reaches its highest value in October and lowest in February. Reflecting on the average monthly electricity prices shown in Figure 4.6c, this behavior can be explained as PtG units refrained from operating at high electricity prices in February while operating the most in October when the average price was the lowest. Moreover, although PtG unit#1 and unit#2 are of the same size, the results in Figure 4.6a show a general trend of unit#1 operating more than the latter. Primarily, this difference in operation is due to the difference in the location of the units connected to the system.

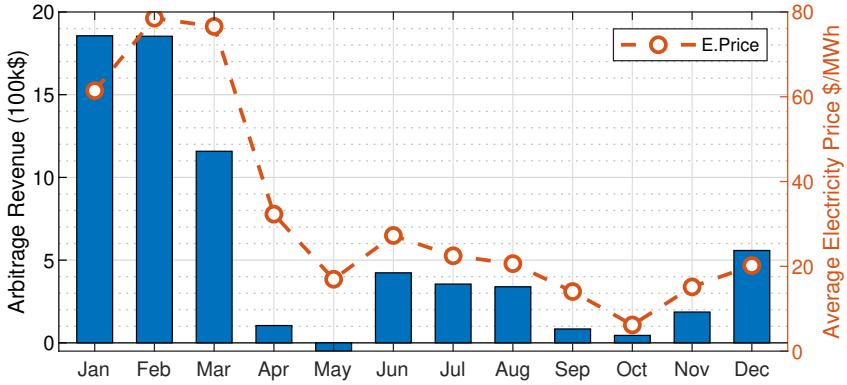
The monthly revenue depicted in Figure 4.6c shows a high correlation with the average electricity price in the associated month. This is due to the way the objective function maximizes the arbitrage by giving the priority to GfG to operate thus selling more electricity at high prices. Noticeably, the average revenue in the month of May is negative, which means that PtG units were forced to operate to absorb surplus energy in the system to maintain the grid balance especially since the system is lightly loaded in that particular month. For the same reason, the revenue is low in April, Sep, Oct, and Nov which are the months among the highest PtG operations.



(a) Monthly PtG units operation



(b) Monthly available renewable energy and system's energy demand



(c) Monthly arbitrage revenue and average electricity price

Figure 4.6: Monthly operation results of the facility at optimal PtG size (32 MW) and $c^{\text{Ren}} = 1500$ illustrating (a) PtG operation, (b) Available renewable energy and system's energy demand, and (c) Arbitrage revenue and average electricity price.

4.4.2 Case Study 2: Comparative Time–of–Use and Wholesale Electricity Price–Based Scheduling in IPGS with Large Renewable Generation

The implication of ToU and wholesale electricity prices for power distribution system applications have been widely studied in the literature [148, 149]. A comparative study between the ToU and wholesale electricity prices and their impact on demand management is conducted in [148]. In [149], an optimal demand-side management approach is proposed to minimize the electricity cost of the industrial sector. The study in [149] compares the wholesale and ToU electricity pricing mechanisms in demand response. The outcomes indicate that the real-time electricity market is preferred as long the consumer responds adequately to the volatility of the electricity prices. The authors in [149] recommend that the ToU pricing mechanism would be desirable for scheduling due to a higher arbitrage opportunity. In [150], the authors propose an algorithm for electricity retailers who participate in demand response programs to bridge the gap between the volatile wholesale and ToU electricity prices. The studies in [150] indicate that it is more robust to procure electricity without uncertainties associated with its prices; that is electricity purchased at ToU rates could be a better option as it follows a consistent trend.

Prior studies on the PtG and GfG scheduling are mainly focused on the scheduling within the wholesale market but not based on the ToU retail prices. A comparative investigation on the scheduling and profitability of the PtG–GfG units based on the ToU and wholesale electricity prices is yet to be performed.

Simulated System

In this section, numerical studies are conducted on the PtG–GfG scheduling model under two approaches as follows: (i) ToU–based and (ii) real-time wholesale price–based scheduling. The IEEE 33–bus power distribution system embedded with a natural gas

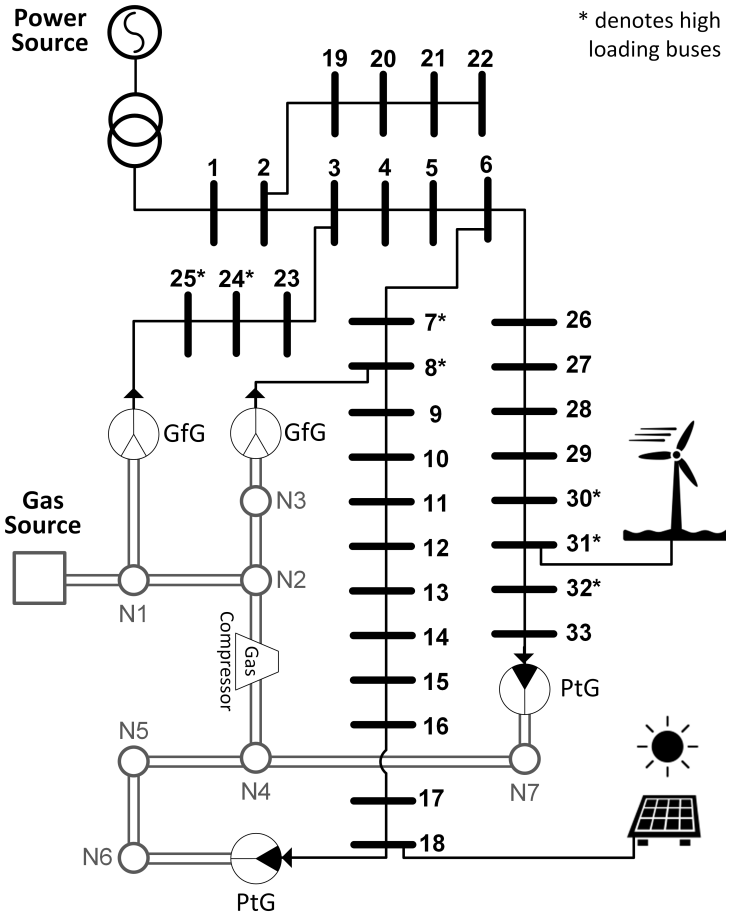


Figure 4.7: Embedded power and natural gas distribution system.

distribution grid is used for numerical studies. It is worth noting that the selected power system has been utilized by prior studies in the literature for numerical evaluation [151, 152]. Figure 4.7 shows the schematic diagram of the test system that is used for the numerical evaluation of the proposed model. As depicted, natural gas and power distribution grids are integrated using two PtG and GfG units. The simulation and modeling parameters are adopted from prior studies in the literature [71, 153].

It should be noted that Ontario's market is taken as the case market. Accordingly, the ToU electricity rates and the wholesale prices in Ontario are selected for numerical studies. Gas prices are considered a time-variant parameter in the model. However, without loss

of generality, a constant value of \$0.174/m^3 is assumed in the case study since currently gas prices are fixed at the distribution level [71].

Power Generation and Demand in Integrated System

Figure 4.8 (a)–(d) show the total generation and demand in the system, including the operation of the PtG and GfG units, for one week out of the studied year. The figure also shows the electricity prices in the wholesale market and ToU rates in the Ontario market. As shown in the figure, wholesale prices are volatile ranging from very low values or negative values to very high peak values. The ToU rates, however, are less volatile and follow a consistent periodic trend. In such a case, there would be more risk and reward if the facility chooses to operate in the wholesale market and experience real-time pricing as compared to the ToU rates. Comparing the operation of the PtG and GfG units under the real-time and ToU price scheduling in Figs. 4.8 (a)–(d), the following outcomes can be extracted:

- The operation of the PtG/GfG facilities is in general volatile under wholesale prices since the facilities track the market price changes. Due to the consistency of the ToU rates, however, the facility shows a more predictable and fairly smooth operation under ToU rates.
- The GfG unit operates considerably more under ToU scheduling as compared to real-time scheduling. This excessive operation is due to higher ToU rates which warrant higher power generation for higher arbitrage benefit. Under real-time scheduling, the GfG tends to operate only at higher market prices to generate arbitrage profit.
- While the PtG is mainly scheduled to operate under lower market prices, this may not always be the case due to the necessity of the PtG unit operation during higher renewable generation. The operation of the PtG unit is needed to eliminate the

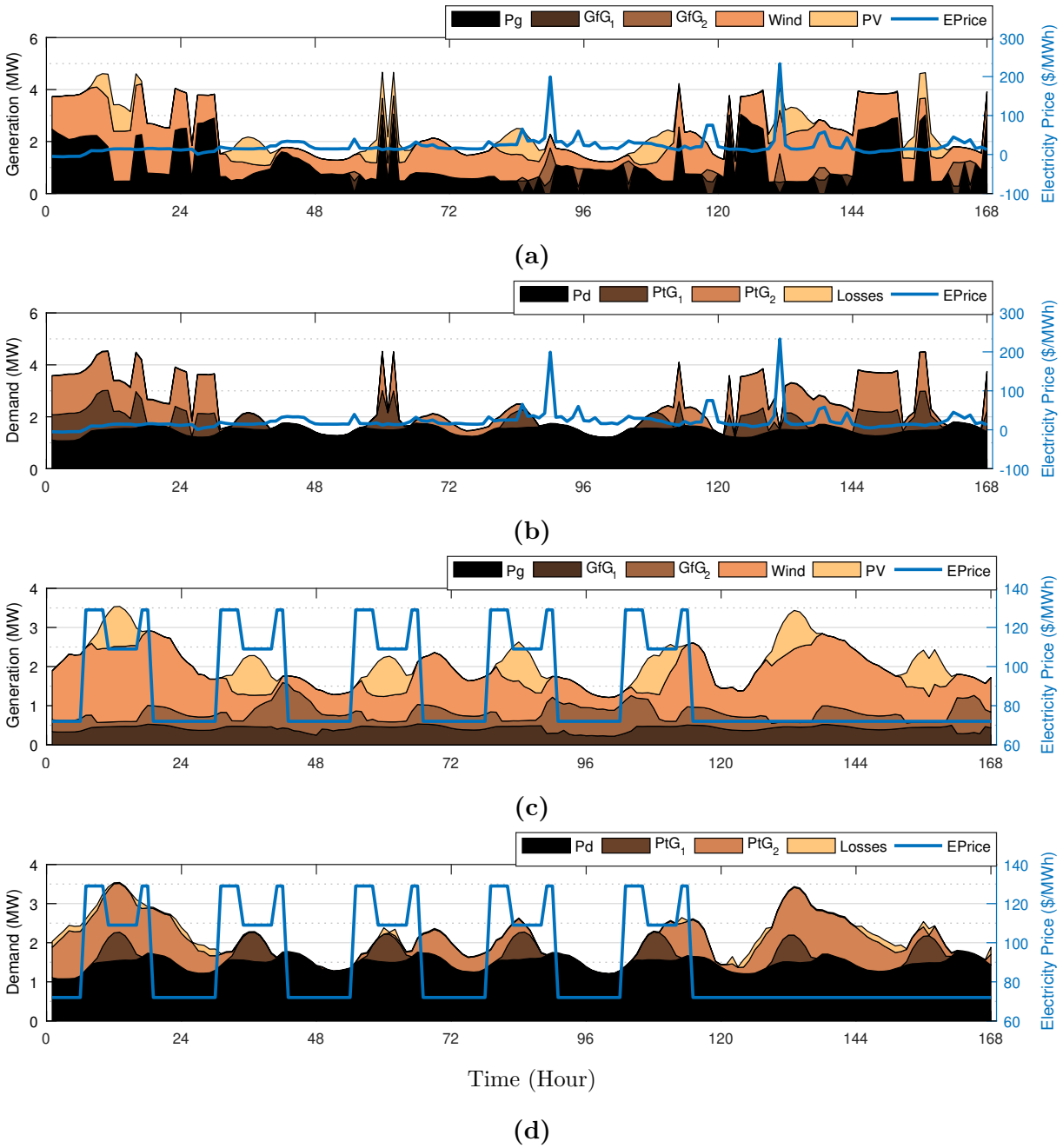


Figure 4.8: System operating parameters under real-time and ToU price scheduling schemes: (a) Power generation under real-time pricing, (b) Power demand under real-time, (c) Power generation under ToU pricing, and (d) Power demand under ToU pricing.

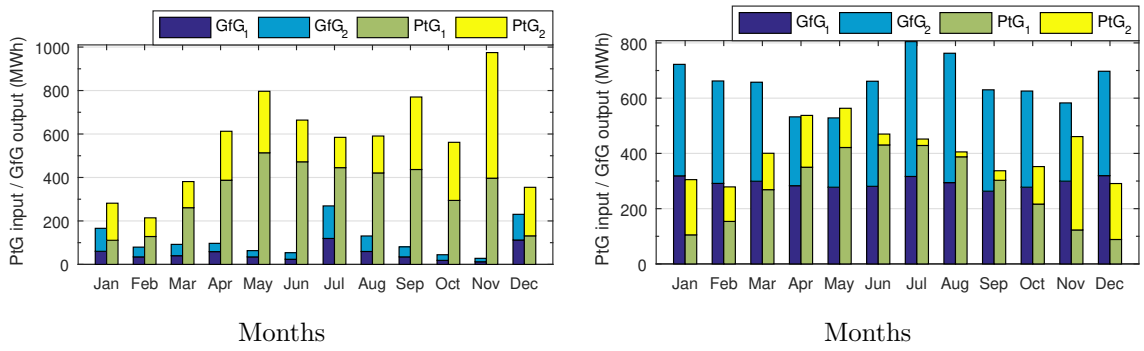


Figure 4.9: Monthly operation of GfG and PtG units for the studied year: *(a)* Under real-time pricing scheme, and *(b)* Under ToU pricing scheme.

surplus renewable generation under both the real-time and ToU scheduling even if this is not economical.

- Power generation which is absorbed from the source is considerably higher under real-time scheduling due to the lower operation of the GfG unit.

The monthly operation of the GfG and PtG units under the ToU and wholesale real-time scheduling mechanisms are depicted in Figure 4.9. As shown in the figure, the GfG unit operates considerably more under the ToU scheduling compared to the real-time scheduling mechanism (3.52 and 4.34 GWh per annum for Units 1 and 2 under ToU scheduling vs 0.61 and 0.73 GWh per annum for Units 1 and 2 under real-time scheduling, respectively). Due to higher values of the ToU rates during several hours of the day, the GfG units reveal considerably higher operations to yield a higher profit. On the other hand, the operation of PtG units is higher under the real-time scheduling due to more arbitrage opportunities at lower market prices (4 and 2.79 GWh per annum for Units 1 and 2 under real-time scheduling vs 3.28 and 1.58 GWh per annum for Units 1 and 2 under ToU scheduling, respectively).

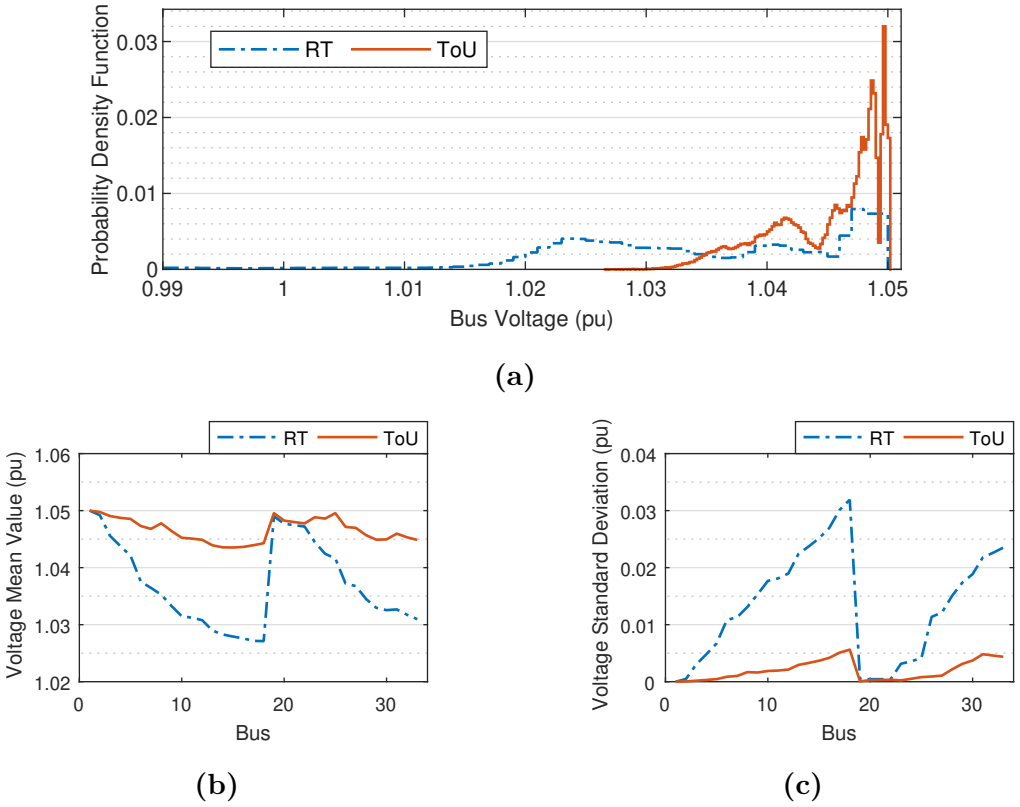
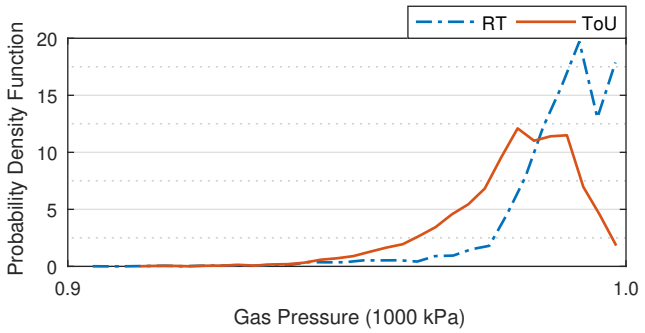


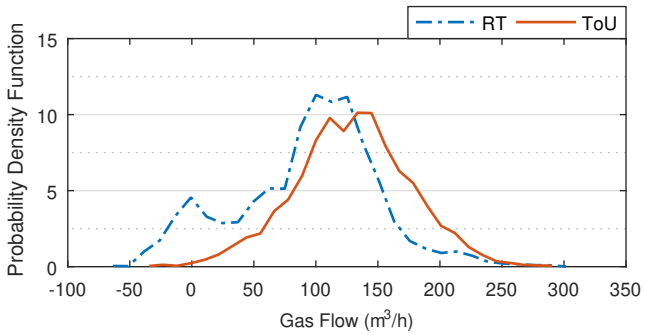
Figure 4.10: Voltage analysis of the 33 buses in the system under real-time and ToU pricing schemes: *(a)* Probability density function (PDF), *(b)* Voltage mean value, and *(c)* Voltage standard deviation.

Operating Parameters of Integrated System

One of the factors that should be taken into consideration is the resilience of the distribution systems under the two cases; i.e., the voltage profile, gas pressure, and gas flow. The Probability Distribution Function (PDF) of the system voltage is computed, and the results are depicted in Figure 4.10 (a). As shown in the figure, the PDF function has a peak of around 1.05 p.u. under ToU scheduling. This indicates that in the majority of the instances, the voltage in the system remains close to the maximum value due to the higher operation of the GfG unit under the ToU scheduling mechanism. The results under the real-time scheduling, on the other hand, indicate that the voltage in the system



(a)



(b)

Figure 4.11: Gas grid pressure and flow analysis under real-time and ToU pricing schemes: *(a)* Pressure probability density function, and *(b)* Flow probability density function.

tends to be lower than the maximum value. As such, the power system has to tolerate higher stress under ToU scheduling due to higher voltage magnitudes.

The mean value and the standard deviation of the system voltages at each bus for a full year are also presented in Figures 4.10 (b) and (c), respectively. As shown in the figures, each bus experiences a different voltage quantity depending on the loading and generation allocations at the bus. In addition, the figure shows that, in general, the system buses are subject to higher voltages under the ToU scheduling compared to the real-time scheduling. This mainly resulted from the higher operation of the GfG unit under ToU scheduling which tends to reinforce the system voltage. The figure also shows that the standard deviation is lower under ToU scheduling due to a more consistent operation of

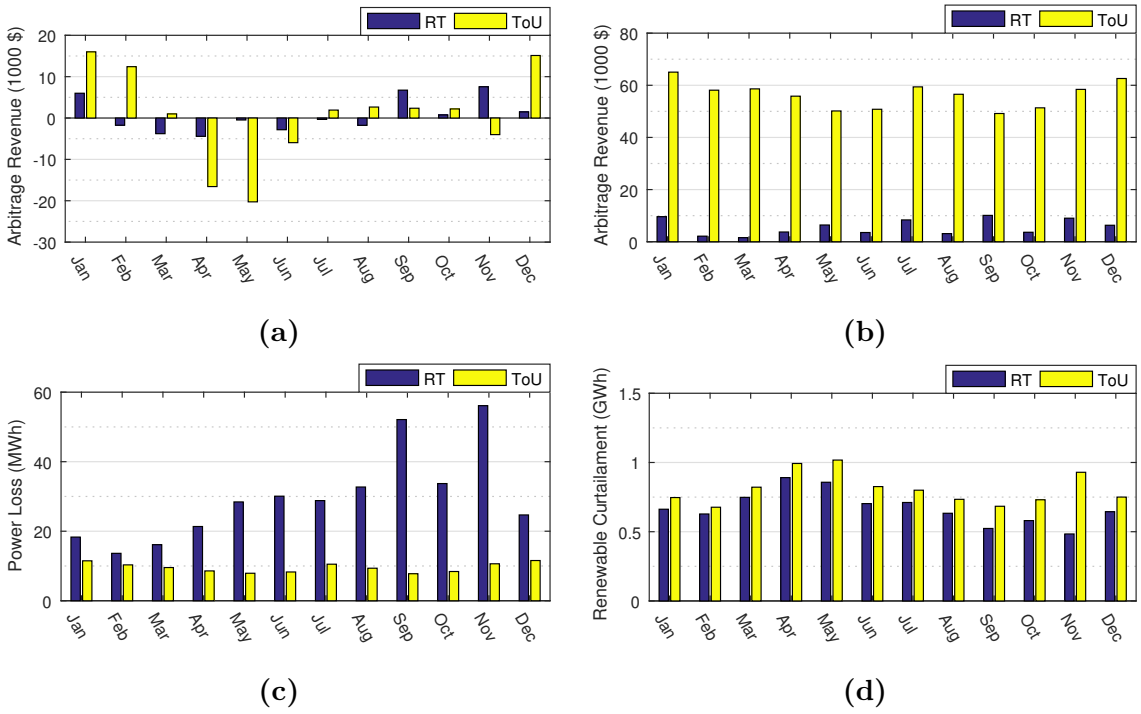


Figure 4.12: Comparing revenue and cost analysis under real-time and ToU pricing schemes: (a) Arbitrage revenue without renewable curtailment, (b) Arbitrage revenue with renewable curtailment, (c) Power losses, and (d) Curtailed power

the PtG and GfG units. This confirms that the voltage is less scattered around the mean value under ToU prices stemming from the fact that the system operation under ToU rates is smoother.

The PDF of the gas pressure and flow are computed, and the results are depicted in Figure 4.11. While the gas pressure profiles under the two scheduling mechanisms are similar, it is slightly lower under the ToU scheduling due to the higher gas consumption of the GfG unit under this pricing scheme. The figure also shows that the peak of the PDF occurs at a similar value for the gas flow under the two scheduling mechanisms, (i.e., around 100 m^3/h). However, the gas flow tends to be negative under the real-time scheduling due to lower gas consumption by the GfG unit and higher gas generation by

the PtG unit, thereby reversing gas flow from downstream to upstream.

Profit Analysis

Figure 4.12 (a) shows the arbitrage revenue resulting from the constrained operation of the PtG and GfG units under the ToU and RT scheduling mechanisms. The operation of the facilities, in this case, is constrained to allow maximum renewable penetration rather than maximum arbitrage benefit. This is realized by setting the curtailment penalty factors $\xi_{j,t}^{PV,Pnl}$ and $\xi_t^{PV,Wnd}$ to very large infinite values to penalize the PV and wind curtailment in the optimization problem. As shown in the figure, the arbitrage revenue is negative for several months under the two scheduling mechanisms, however, the total revenue is positive at \$7.15 k and \$6.87 k per annum for real-time and ToU scheduling, respectively. This is due to the higher renewable penetration which causes the operation of the PtG units during the periods when such operations are not economical. As such, the PtG units would have to be operated less than optimality to allow higher penetration of renewables.

Figure 4.12 (b), on the other hand, shows the case where the facilities are operated in the unconstrained mode, i.e., minimum renewable penetration, but maximum arbitrage benefit. The penalty factors $\xi_{j,t}^{PV,Pnl}$ and $\xi_t^{PV,Wnd}$ are set to 0 values, in this case, to allow the optimization problem to curtail the renewable penetration as needed to maximize the arbitrage revenue. As shown in Figure 4.12 (b), scheduling under the ToU rates results in a considerably higher profit as compared to the real-time scheduling (\$676.09 k under ToU scheduling vs \$67.5 k under real-time scheduling). As noted earlier in this chapter and evaluated through the numerical results, this is due to higher ToU rates, thereby higher financial opportunities for the GfG facility to generate power and sell to the power market. Figure 4.12 (c) shows that higher losses are introduced under real-time scheduling due to less local generation, and thus, higher power flow from the source to the load (356.1 MWh under real-time scheduling vs 114.39 MWh under ToU scheduling). The higher operation of the GfG facility, however, results in smaller renewable penetration or higher renewable curtailment as shown in Figure 4.12 (d) (9.71 GWh curtailment under ToU scheduling vs

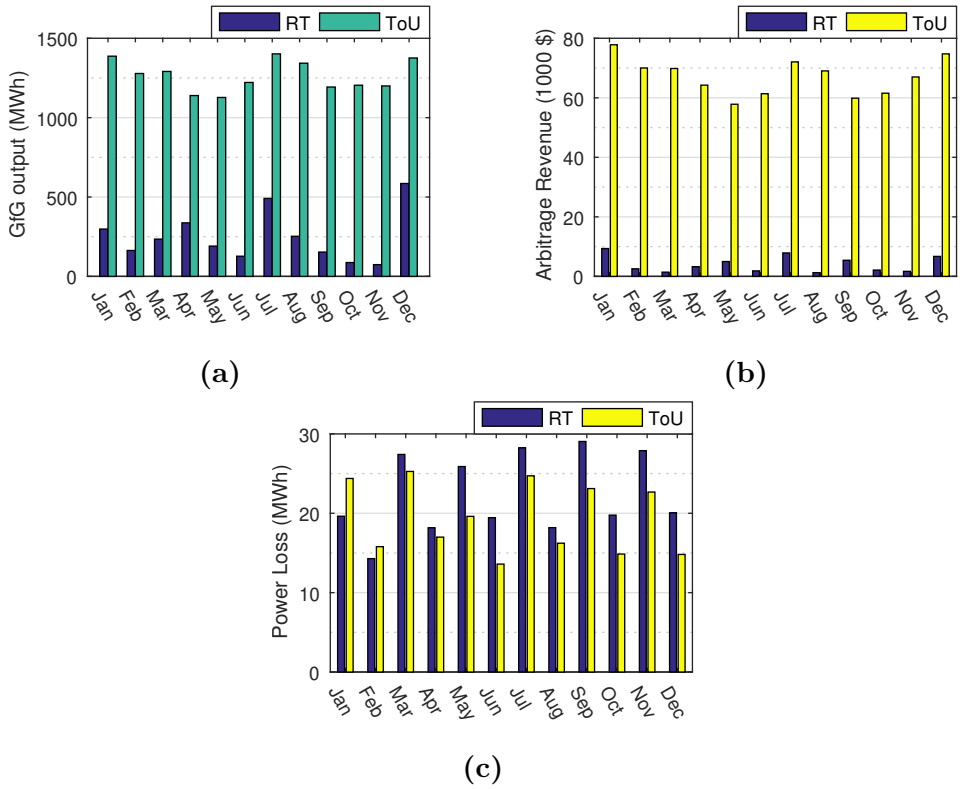


Figure 4.13: Operating parameters with GfG unit only under real-time and ToU scheduling schemes: *(a)* GfG output power, *(b)* Arbitrage revenue, and *(c)* Power loss cost

8.07 GWh curtailment under real-time scheduling). As such, while the facility generates a higher arbitrage benefit under the ToU scheduling, it would limit the penetration of renewable generation and causes more losses in the system.

GfG Operation Only

The joint operation of the PtG and GfG units are evaluated in the above sections. In this section, the operation of the GfG unit only (i.e., no PtG unit) is evaluated, and the results are presented in Figure 4.13 (a)–(c) under no renewable energy curtailment. As expected, the GfG unit shows considerably higher operation under ToU scheduling due to higher ToU rates (15.16 vs 3 GWh). In addition, Figure 4.13 (b) represents that the monthly arbitrage revenue is significantly higher under ToU scheduling, mainly due to

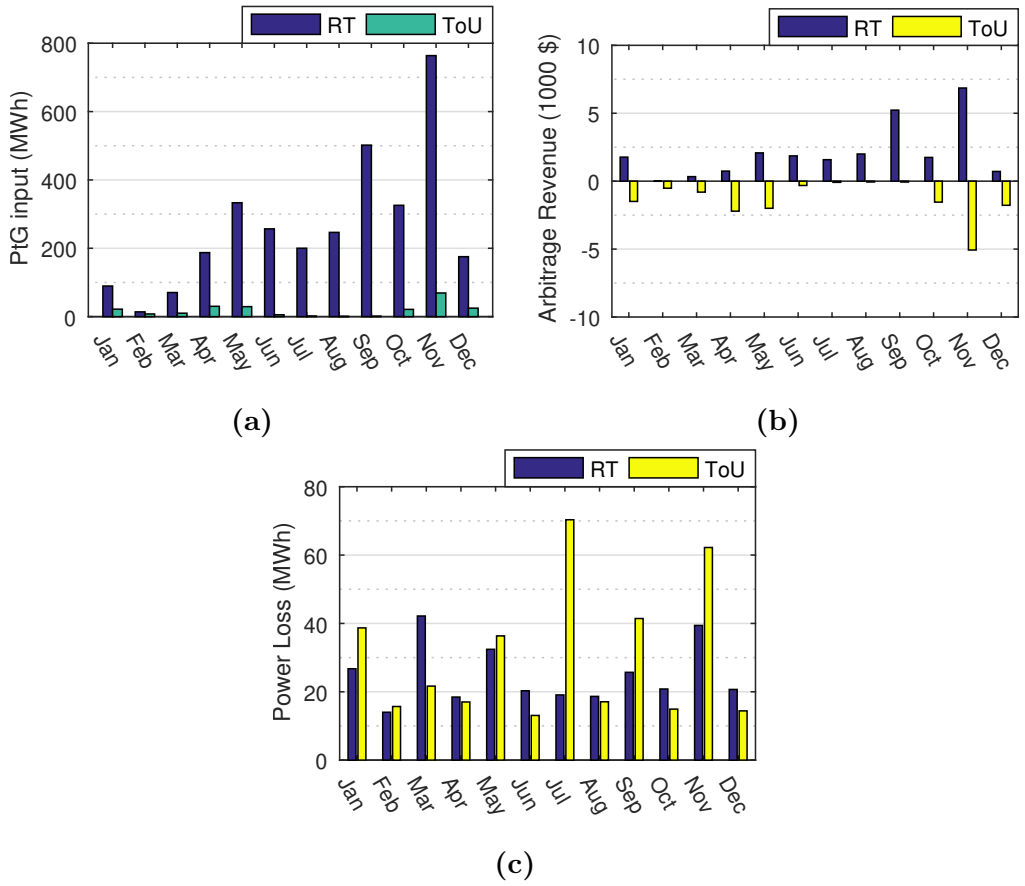


Figure 4.14: Operating parameters with PtG unit only under real-time and ToU scheduling schemes: *(a)* PtG input power, *(b)* Arbitrage revenue, and *(c)* Power loss cost.

higher ToU rates ($805.45 k vs $48.55 k). The system losses under real –time scheduling are slightly higher than the losses under ToU (268.02 vs 232.07 MWh). Consequently, in cases where only the GfG unit is scheduled (not jointly operated with the PtG unit), ToU scheduling offers considerably higher financial benefit for the operation of the GfG unit.

PtG Operation Only

Figure 4.14 (a)–(c) represents the operating results for the case where only the PtG unit is utilized (not jointly operated with the GfG unit), under no renewable energy curtailment. As shown in the figure, the PtG unit exhibits a considerably higher operation under real-

time scheduling than the ToU scheduling (3.16 GWh vs 223.34 MWh). This mainly stems from the fact that the operation of the PtG unit is not economical at higher ToU rates. The PtG unit, under ToU scheduling, mainly operates to eliminate the surplus renewable generation, thereby causing negative arbitrage revenue as depicted in Figure 4.14 (b), i.e., −$15.94 k. Under real-time scheduling, on the other hand, the PtG unit actively operates at lower or negative market prices to generate arbitrage revenue. Accordingly, the arbitrage revenue shows a variable monthly, but mainly positive trend as depicted in Figure 4.14 (b), i.e., $24.92 k. In addition, a clear correlation between the amount of operation and the arbitrage revenue can be observed under real-time scheduling; the higher the PtG unit operates, the higher the arbitrage revenue would be. Figure 4.14 (c) indicates that the systems losses under the two scheduling mechanisms are similar under the two scheduling mechanisms (362.9 vs 298.425 MWh under ToU and real-time scheduling, respectively).

As noted above, the PtG unit mainly generates profit at lower values of wholesale market prices. In order to reveal the impact of market price values on the revenue of the PtG unit, the market price values for the studied year are analyzed. Table 4.1 reports the number of hours with low and peak prices, in addition to the sum of the prices during those hours. It is worth noting that the lower and upper market prices are defined as the prices below and above the lower and upper interquartile range (IQR), respectively. For the studied year, the lower and higher prices fall below 2.72 $/MWh and above 47.3 $/MWh, respectively. Comparing the arbitrage profit in Figure 4.14 (b) and the results in Table 4.1, one can realize that there is a strong correlation between the number of hours under the lower IQR and the monthly arbitrage revenue. The higher the number of hours under lower IQR is for a given month, the higher the arbitrage revenue would be. This is mainly because higher instances of low prices provide higher financial opportunities for the PtG unit under real-time scheduling.

Table 4.1: Wholesale electricity price analysis

	Upper Interquartile Range		Lower Interquartile Range	
Months	Hours	Sum of Prices ($/MWh)	Hours	Sum of Prices ($/MWh)
Jan	64	6059.5	13	–560.79
Feb	30	2168.2	0	0
Mar	17	1019.4	8	2.17
Apr	38	2648	18	–37.76
May	36	3968.9	42	–92.87
Jun	19	1485.5	33	–108.26
Jul	63	5569.6	30	–84.86
Aug	20	1274	46	–127.54
Sep	27	3439	107	–340.67
Oct	18	1602.3	33	–18.91
Nov	15	1303.9	135	–388.58
Dec	59	4272.2	13	2.74

4.5 Summary and Discussion

In this chapter, a framework for the joint operation of PtG and GfG facilities within IPGS is presented. Two case studies are conducted to validate the framework considering renewable energy penetration on transmission and distribution systems. In the first case study, the PtG units are sized based on the unit's utilization rate within one year of

operation. The approach is evaluated on the IEEE-30 bus transmission system and the Belgian gas network using real-world historical data. Results show a consistency in the optimal size selected when varying renewable energy penetration enforcement factors. The facility's monthly operational results are discussed and explained.

The second study presents comparative ToU and wholesale price–based scheduling from the economic point of view under different operational scenarios. Both the individual and joint scheduling of the PtG and GfG facilities are assessed under the ToU and wholesale market prices. The numerical evaluations are performed to investigate the performance of the proposed model on a test system using real-world operating data. It is demonstrated that the joint operation of the PtG and GfG units can help balance the generation and demand in the system by injecting power to the high load area and absorbing the surplus renewable generation from the high generation area. Higher renewable generation, however, could limit the operation of the GfG unit, thereby impacting the arbitrage revenue achieved by the PtG and GfG units. The results indicate that the joint operation of the PtG and GfG units could result in higher arbitrage values under ToU scheduling, but more renewable curtailment and more system losses. In cases where only the GfG unit is scheduled, ToU rates could offer a considerably higher arbitrage benefit to the operator of the GfG unit. On the other hand, real-time scheduling could result in a more stable arbitrage benefit if only the PtG unit operates. The results also demonstrate that the higher the instances of lower market prices are, the more the arbitrage revenue of the PtG unit would be, under the real-time scheduling.

Chapter 5

Develop Intelligent Detection Approach for False Data Injection Attacks against Power and Gas Systems Integration Facilities

In Chapter 4, a framework for the joint operation of Power–to–Gas (PtG) and Gas–fired Generation (GfG) facilities is presented. In such an integrated system, where critical operating information and control signals of both systems need to be communicated, the risk of cyber–attack is intensified. This chapter presents a new attack model on the PtG and GfG integration facilities of power and gas systems. Initially, it demonstrates how the operation of the integrated system can be adversely impacted during cyber–attacks that may not be detected using traditional methods. Next, two new detection schemes are proposed for False Data Injection Attacks (FDIAs) against the input and output signals of the PtG/GfG facility scheduler. In the first scheme, a supervised machine-learning technique, based on Convolutional Neural Network (CNN) and wavelet transforms, is adopted to detect attacks on the information received by the facility scheduler. In the second scheme, a hybrid neural network is developed, based on an unsupervised learning

technique, that requires no labeled training information to detect attacks on the output control signals issued by the scheduler. In both schemes, information acquired from local sensors and deterministic estimation methods is utilized for signal evaluation. The proposed schemes are incorporated into the facilities' scheduler to create a cyber–attack resilient scheduling model in an integrated power and gas grid. Lastly, the efficacy and feasibility of the proposed model are evaluated via numerical studies using the IEEE30-bus power system integrated with the Belgian gas grid as the test bed using historical operating parameters.

5.1 Introduction

The vast integration of advanced Information and Communication Technologies (ICT) infrastructure into various energy systems has offered a framework for efficient utilization of multiple energy forms [154]. Under this umbrella, researchers have been recently investigating the utilization of natural gas grids to deal with the intermittency of renewables [3]. Despite the potential advantages of integrated energy systems, this extensive dependency on digital communication has also made such systems vulnerable to cyber–attacks [9]. For instance, an attack on the data provider of three U.S. natural gas pipeline companies in April 2018 caused a service shutdown for several days [155]. The cyber–attacks against energy systems are identified as major national security threats [156, 157]. To that end, an investigation is required on FDIAs as a significant type of data integrity breach capable of disrupting the operation of modern power systems [87] and industrial controllers [99]. Consequently, as the grid operators decide to integrate gas and power networks to form multi–carrier energy systems, new measures for securing the integrated grids against FDIAs are yet to be implemented.

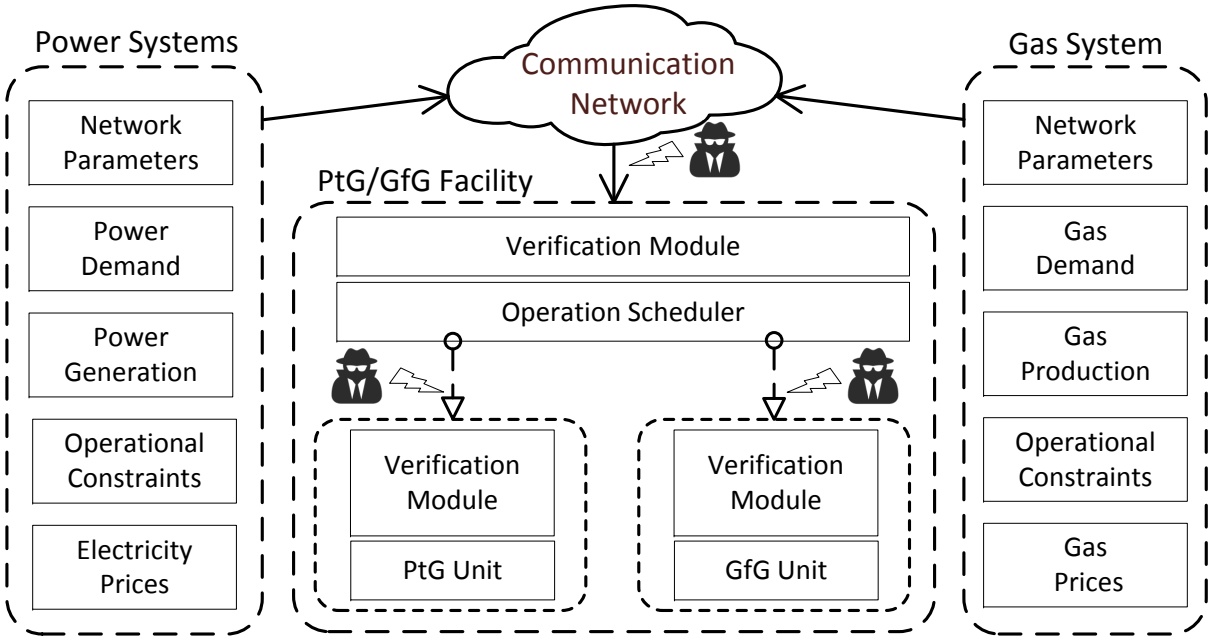


Figure 5.1: Framework for development of cyber–attack resilient scheduling model in an integrated power and gas transmission system.

5.2 Problem Description and Hypothesis

The two–way energy conversion within the integrated system, through PtG/GfG facilities, allows flexibility in operation that would balance out the loading and generation levels, and thus contributes towards increasing the renewable energy penetration level into the grid. In such a case, any interruption or misoperation of the PtG/GfG facilities would impact the success of the system and even endanger the security and reliability of the integrated grids. The focus is mainly on the interruptions occurring due to FDIA on the information/signals exchanged between the central controllers and energy sources in the integrated grid. In particular, the method proposed in this chapter aims to equip PtG/GfG facilities with detection schemes to maintain the resiliency of the entire integrated system.

The proposed framework for the development of an attack resilient scheduling model

in an integrated power and gas transmission grid is illustrated in Figure 5.1. As shown in the figure, information regarding the network parameters and operational constraints is communicated to the PtG/GfG facility scheduler. The power/gas demand, generation levels, and electricity/gas prices are also sent to the scheduler while updated in real-time through communication networks, e.g., the Internet, which is susceptible to cyber–attacks. Such information, referred to as primary data in this proposed method, is utilized by the scheduling model to decide the optimal setpoints of the PtG/GfG units. It is assumed that PtG and GfG facilities are dispersed throughout the grid and are scheduled by a central controller managed by a single entity (e.g., gas grid operators or private investors); hence, the scheduling signals, referred to as secondary data, would be sent out to the PtG/GfG units via a wide-area communication network or the Internet. In such a setup, both primary and secondary signals are subject to potential cyber–attacks; attacked signals would cause operational and instability issues in the integrated grid.

The proposed method aims to address the cyber-security issues in the above-described framework via verifying both the primary and secondary signals. The proposed model comprises two modules: (i) primary data verification module to verify the information external to the control facility, which will be fed to the scheduler, and (ii) secondary data verification module placed at the PtG/GfG unit locations aiming to verify the operational setpoints received from the central controller. Accordingly, building on the optimal scheduling algorithm presented in Section 4.3, the proposed verification model is presented the following section.

5.3 Cyber-Attack Detection Model

As mentioned earlier in Section 5.2, the proposed attack–resiliency model comprises primary and secondary data verification modules. The steps for developing these two modules are illustrated in Figure 5.2. Initially, (1) historical data of the integrated system are collected and stored in a dataset. Besides, the network parameters and constraints needed

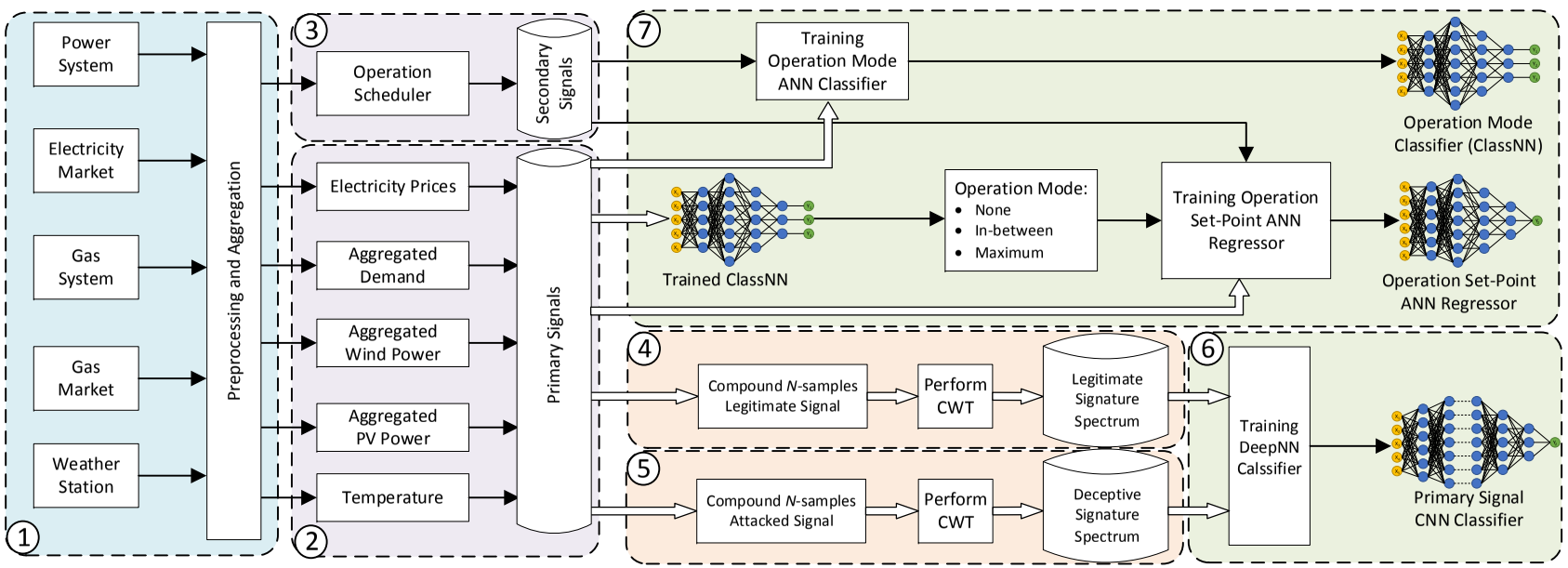


Figure 5.2: Flowchart of the proposed model for primary and secondary signals verification to protect the IPGS against cyber–attacks.

for scheduling, other parameters include the hourly values of electrical load at each bus, electricity prices, wind and Photovoltaic (PV) generation, gas prices, gas demand, and production at each node in the gas grid, and temperature are also collected. (2) These parameters are aggregated and stored in the primary signals dataset. In addition, (3) the scheduling data of the PtG and GfG facilities are collected and stored in the secondary signals dataset.

The primary data are, then, (4) passed through Continuous Wavelet Transforms (CWTs) to generate spectrum in the frequency domain, and the results are stored in a dataset named *legitimate signature spectrum dataset*. As shown in Figure 5.2 (5), in addition to the legitimate data, various attack scenarios on the primary data are simulated and passed through CWTs, and the results are stored in a *deceptive signature spectrum* dataset. The respective attack scenarios are chosen to simulate the behavior of a mindful attacker who modifies the signals in such a way that the attack cannot easily be detected by normal error checking methods (e.g., maintain PV generation as zero during nighttime periods). Next in step (6), a CNN network is trained with a training dataset excerpted randomly from both the legitimate and deceptive signature spectrum datasets along with their corresponding classes. (7) Along with the development of primary data verification, both primary and secondary signals are utilized to train neural network models to detect the operation mode and the validity of the scheduling data. Further elaboration in this regard is given in the below sections. It is worth noting that multiple cross-validation rounds are performed and a separate dataset for testing is taken to avoid data overfitting during the training of the models.

5.3.1 Detecting Attacks on Primary Signals

The process for the creation of the primary data verification model is given in this section. In general, five primary signals are considered for verification as shown in Figure 5.3, which are categorized into the following:

Type 1: Signals that are received from the sources local to the PtG/GfG unit location,

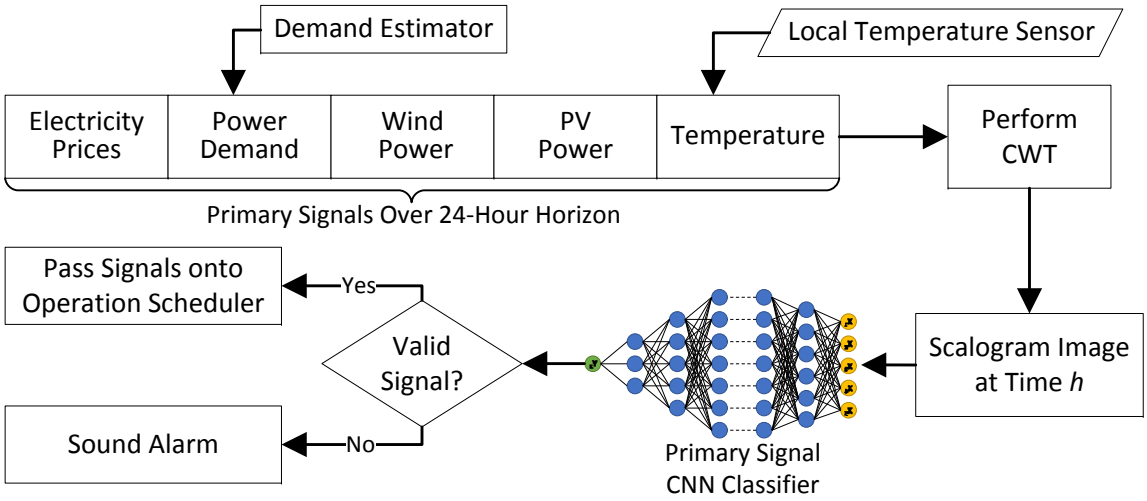


Figure 5.3: Flowchart of verifying primary signals received from external sources.

e.g., temperature acquired from a local sensor at the facility location. This type of signal is considered secure, thereby no need for additional verification other than error checking.

Type 2: Signals that are received from the sources external to the PtG/GfG unit location can be intercepted and tampered with by an attacker, e.g., market prices and wind/PV power. These signals require to be passed through a robust verification model to detect and block the data fabricated by cyber–attacks.

Type 3: Signals that are estimated using the historical data, e.g., the total power demand as will be explained later in this subsection.

A verification model is formulated as a binary classification problem using CWT and CNN structure. The complete process of verifying primary signals received from external sources is shown in Figure 5.3. At any time step t, a compound signal of N-samples is created composed of the historical primary data over the last 24 hours, e.g., electricity price, power demand, wind/PV power, and temperature. The CWT is, then, applied to this compound signal to extract a scalogram spectrum represented as an image that would act as the signature of the signal in the time and frequency domains. An example of the signal and its CWT signature spectrum image is shown in Figure 5.4. The signature image is then input to the trained CNN, which determines if it is legitimate. It is worth

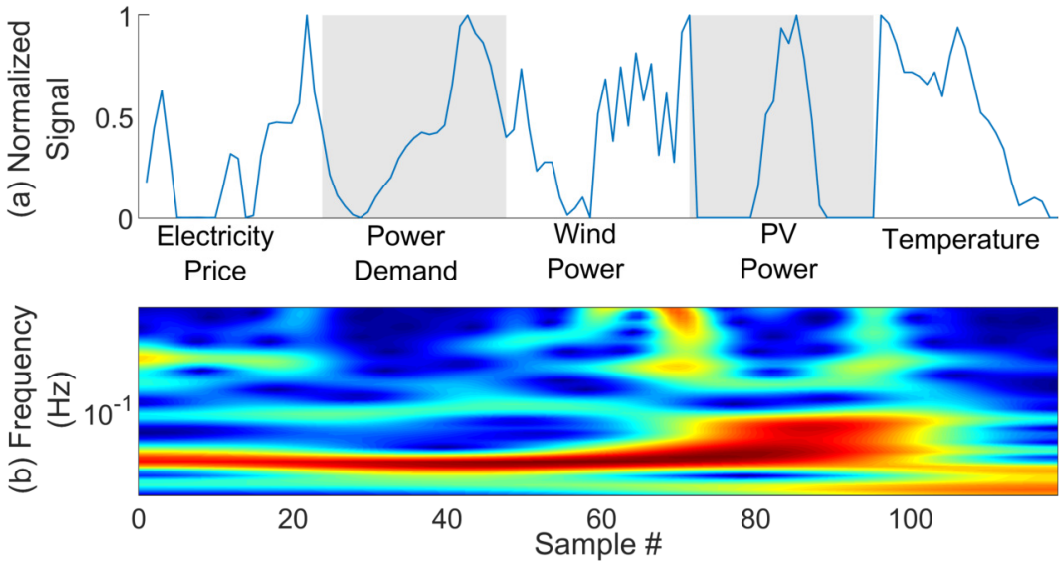


Figure 5.4: Compound primary signals: (a) Normalized values, (b) Frequency components acquired using CWT.

noting that different CWT parameters generate different spectra; however, this does not impact the validity of the model as long as the same parameters are utilized during both the training and verification phases. Legitimate signals are passed onto the operation scheduler, while the deemed attacked signals are either blocked or an alarm is sounded notifying the operator for further investigation.

Demand Estimation

Electric power demand belongs to *Type 3* signals as mentioned above, i.e., estimated using local information rather than data received via the communication medium. As such, a demand estimation model would require to be developed and integrated into the verification model, which is employed for demand verification. The aggregated electric demand $P^{\mathrm{D}}_{\mathrm{agg},t}$, i.e., the total demand on the system buses, in power systems usually follows a periodic pattern on a daily, weekly, and seasonal basis. Given this periodic nature, the Fourier series can be employed to represent the demand as follows:

$$P^{\mathrm{D}}_{\mathrm{agg},t} = a_0 + \sum_{n=1}^{N} a_n \cos(\omega_n t) + \sum_{n=1}^{N} b_n \sin(\omega_n t), \tag{5.1}$$

where N represents the order of the harmonics and the coefficients a_0, a_n, and b_n are all unknown parameters in the model and their value is to be determined based on the analysis of the historical demand data. The frequency of the electric demand, ω_n, is given in the following equation:

$$\omega_n = 2\pi n f \quad \forall\, n \in \{1, 2, 3, \cdots, N\}, \tag{5.2}$$

given the Fourier series format in (5.1), (5.2) infers that the electric demand signal can be represented through the fundamental frequency f and a set of harmonics n. Consequently, (5.1) can be expressed in the matrix form as follows:

$$P^{\mathrm{D}}_{\mathrm{agg},t} = \mathbf{D}(t) = \mathbf{C}.\mathbf{H} + \mathbf{e} \tag{5.3}$$

$$\mathbf{H} = \ [1, \cos(w_1 t), \ldots, \cos(w_n t), \sin(w_1 t), \ldots, \sin(w_n t)]^{tr} \tag{5.4}$$

$$\mathbf{C} = \Big[a_0, a_1, \ldots, a_N, b_0, b_1, \ldots, b_N\Big]. \tag{5.5}$$

The least-square error-based method can be used to determine the unknown parameters and coefficients in (5.5). Using matrix conversion techniques, (5.3) is further expanded into the following:

$$\mathbf{C}^{tr}\mathbf{H}^{tr}\mathbf{H}\,\mathbf{C} - 2\,\mathbf{C}^{tr}\mathbf{H}^{tr}\mathbf{D}(t) + \mathbf{D}(t)^{tr}\mathbf{D}(t) = \mathbf{e}^{tr}\mathbf{e}. \tag{5.6}$$

Finally, deriving (5.6) with the unknown set as the matrix $\mathbf{C}$ and setting the derivative to zero, yields the value of matrix $\mathbf{C}$ that minimizes the error $\mathbf{e}$; accordingly, $\mathbf{C}$ can be expressed as,

$$\mathbf{C} = \Big[\Big[\mathbf{H}^{tr}\,\mathbf{H}\Big]^{-1}\,\mathbf{H}^{tr}\Big]\,\mathbf{D}(t). \tag{5.7}$$

Training Data

For the development of the initial attack detector, historical real-world primary data and the synthetic false data can be utilized for training the supervised CNN-based cyber–attack detector. Ideally, such training data shall include information acquired from real-normal and real-attack scenarios extracted from historical records. However, due to the

relative scarcity of such real data especially for PtG and GfG facilities, synthetic attack scenarios can be utilized to enrich the training datasets to construct the initial detector. The synthetic false data is carefully selected to include various attack severity levels as determined by the mismatch between the false and legitimate signals. This training data enrichment method has been adopted in previous research works on cyber attack detection using machine learning approaches [97–99, 101]. For instance, in [97], the authors generate synthetic compromised data using the Fourier transform, principal components analysis, and computational methods. In practice, adversaries potentially will follow similar approaches to construct attack vectors in order not to trigger the detection mechanism [100]. Eventually, the performance of the detector can be improved in the post-deployment phase by continuously training the detector using real normal and attack data once they become available.

5.3.2 Detecting Attacks on Secondary Signals

Using primary and secondary datasets, a typical regression neural network model (RegNN) can be trained to estimate the operation (i.e., scheduling) setpoints of PtG/GfG units. Furthermore, conducting a frequency analysis over the scheduling data for a full year reveals the following three dominant operation modes:

– *None*: PtG/GfG unit does not operate.

– *In–between*: the operation setpoint signal is above zero, but less than the rated capacity of the PtG/GfG unit.

– *Maximum*: the PtG/GfG unit operates at the rated capacity.

Consequently, a hybrid regression model (C+RegNN) to enhance estimation accuracy is proposed by including the output of an additional three–class neural network classifier as input to the regression model along with the primary and secondary signals. The classifier estimates the operation mode of the PtG/GfG units as one of the three aforementioned modes.

The steps for verifying the operation setpoint signals are depicted in Figure 5.5 com-

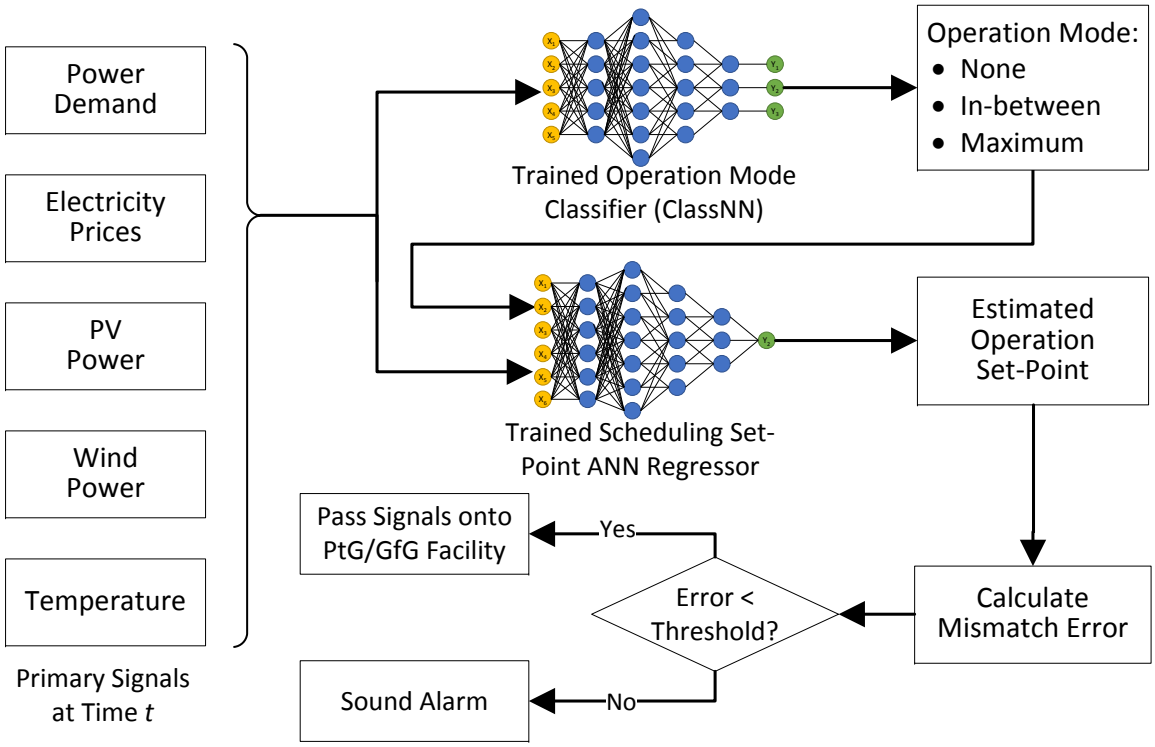


Figure 5.5: Verifying secondary signals received from the central controller.

prising the hybrid C+RegNN model. As shown in the figure, the output of the C+RegNN is compared with the received setpoint signal to calculate the mismatch error. Then, an alarm is sounded when the mismatch level is above a preset alarming threshold; otherwise, the secondary signal is accepted and passed onto the PtG/GfG unit for operation. Finally, during the initial development of this detector, synthetic secondary data are utilized for training the machine learning detectors. Since the proposed detector is unsupervised, only the normal data are used for training that would eliminate the need for generating synthetic false control information. Eventually, the performance of the detector can be improved after deployment by continuously training the detector using real normal and attack data once they become available.

5.4 Case Studies and Discussion

In this section, the integrated system with PtG–GfG units shown in Figure 5.6 is utilized as a platform for conducting numerical studies on the proposed scheduling model and attack detection approaches. The integrated system comprises the IEEE–standard 30–bus power transmission system [158] coupled with a modified version of the 20–node Belgian gas transmission grid which has been widely used to study the integrated power and gas systems [30, 147]. First, a case study is presented to demonstrate the operational results of the proposed scheduling model during both the normal and attack conditions. Then, the performance of the proposed FDIA detection mechanism is evaluated by presenting two case studies considering the attacks on both the primary and secondary signals. The experiments are implemented in the MATLAB software environment, and the results are analyzed.

5.4.1 Impact of Attacks on the Facility Operation

Real-world historical operating data of electrical and gas loads, and PV and wind power generation are utilized for the study. The historical hourly prices of Ontario's electricity market are utilized, whereas the gas price is considered fixed at the rate of \$0.174/m^3 [68]. The modeling and operational parameters of the PtG/GfG facility are adopted from [68], where Table 5.1 reports the main parameters used for the study; in which Hourly Maintenance Cost (HMC) indicates the hourly maintenance cost.

1) Attack Model: The FDIA against the facility scheduler is simulated considering a model referred to as the man-in-the-middle attack model with the following two basic assumptions regarding the attacker's capabilities:

1) the attacker is capable of corrupting the primary data received from the power and gas systems, and/or the secondary data sent to the PtG/GfG units by the scheduler,

2) the attacker is able to mask any feedback returned to the facility controller regarding the current scheduling setpoints of PtG/GfG facilities.

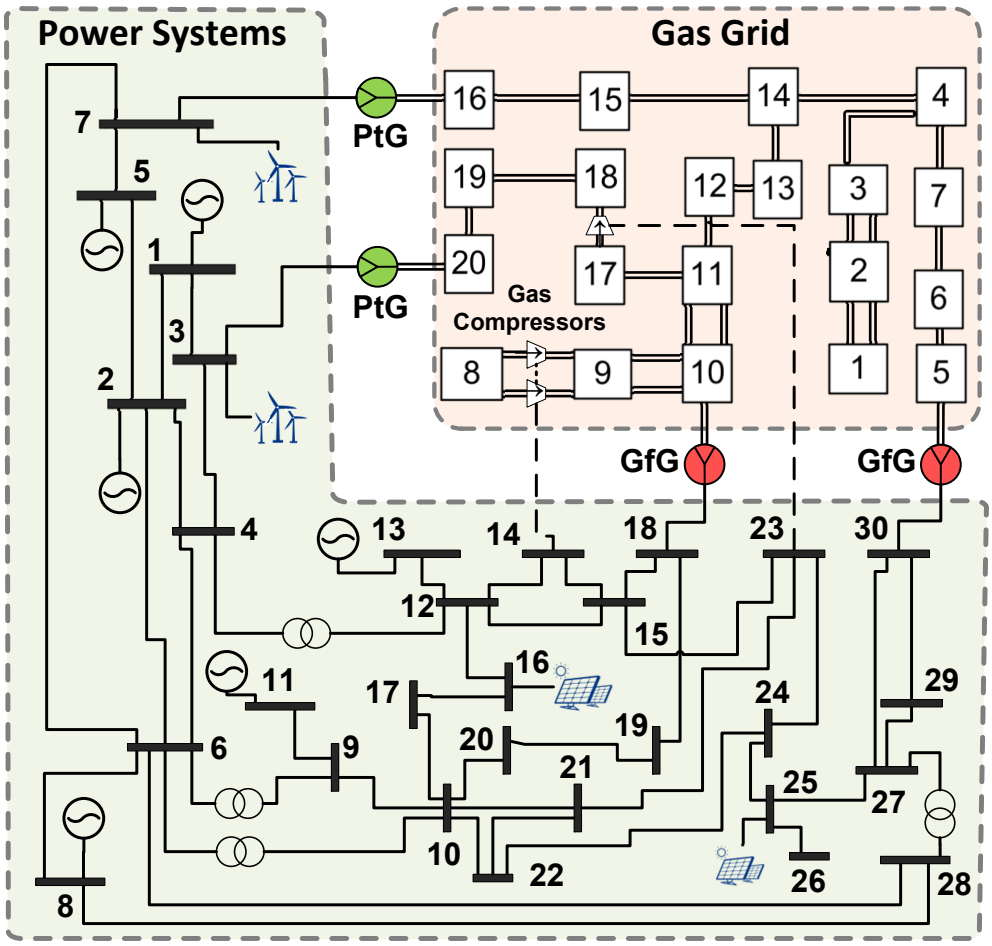


Figure 5.6: 30–bus IEEE-standard power transmission system integrated with a 20–node gas transmission grid employed for numerical studies.

Table 5.1: Simulation and Modeling Parameters

$\Delta t = 1$ (h)	$\boldsymbol{\mathcal{T}} = 8760$ (h)
$\overline{P}^{\mathrm{PtG}} = 30$ MW	$\overline{P}^{\mathrm{GfG}} = 30$ MW
$\alpha = 94.7$ MWh/m^3	$\beta = 1/94.7$ m^3/MWh
$\mathtt{C}_j^{\mathrm{PtG}} = 30\% \times \mathrm{HMC}/\overline{P}_j^{\mathrm{PtG}}$	$\mathtt{C}_j^{\mathrm{GfG}} = 70\% \times \mathrm{HMC}/\overline{P}_j^{\mathrm{GfG}}$
CAPEX = \$49.8 Million	Facility Age = 20 years = 175200 (h)
HMC = 0.5%×CAPEX / Facility Age	

In addition to the above-mentioned assumptions, the aggressive and non-aggressive types of attack scenarios are distinctly considered in this chapter based on the attack's understanding of the scheduling model:

1) Non–aggressive attacks where the attacker intercepts the signals received/sent by the central controller and replaces them with some false data; if successful, this may not significantly impact the operational setpoints of PtG/GfG units and the integrated system but causes financial losses for the system. This type of attack is normally performed when the attacker lacks information/knowledge about the operational mechanism of the scheduler.

2) Aggressive attacks where the attacker injects false signals to adversely alter the operating points of the system that would cause such issues as system overloading, e.g., flip PtG/GfG unit setpoints between the maximum and minimum values.

In both scenarios, the attackers are assumed to inject false signals that are not easily discovered by the traditional Bad Data Detection (BDD) mechanism, e.g., injecting false PV generation level to deceive the scheduler only during the daytime.

In order to demonstrate the impact of cyber–attacks on the operation of the integrated system, the monthly aggregated profiles of the system parameters are computed and

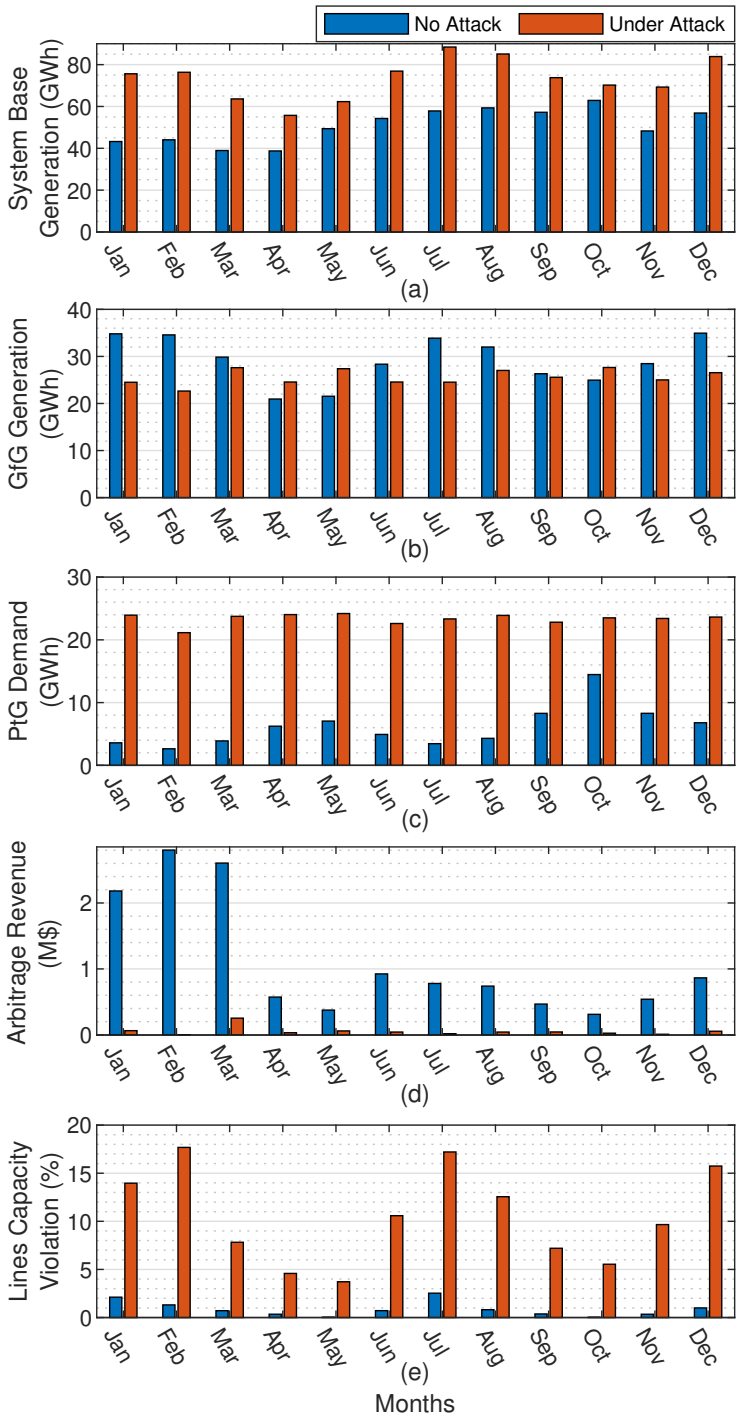


Figure 5.7: Monthly operating of PtG/GfG facilities: (a) Base generation, (b) GfG generation, (c) PtG demand, (d) Arbitrage revenue, and (e) Lines capacity violation.

represented in Figure 5.7 (a)–(e). The results are computed considering both normal conditions and non-aggressive attack scenarios as shown in the figure. Figure 5.7 (a) shows that the total base–power generation, captured at the slack bus, increases from 610 GWh during the normal condition to 810 GWh during the attack. Figure 5.7 (b) shows that the total power generation from the GfG units drops from 350 GWh during normal conditions to around 300 GWh during the attack. Conversely, the total power demand of PtG units significantly increases from 74 GWh during normal conditions to 280 GWh during the attack as shown in Figure 5.7 (c). As such, the attack in the PtG/GfG scheduling signals has caused substantial elevation in the system base generation. Figure 5.7 (d) shows that the total system revenue has remarkably declined from 13 M$ during normal conditions to less than 1 M$ under the attack scenario. Besides, the uncontrolled system conditions during the attack have endangered the system stability by substantially overloading the lines, as shown in Figure 5.7 (e).

5.4.2 Aggressive Attacks without Detection Model

In this scenario, it is assumed that an adversary gains access to tamper with the secondary signals of the PtG units. To cause devastating damages, the attacker performs an aggressive attack by inverting the operating signals, i.e., running the PtG unit when it is supposed to be off and vice–versa. In this case, it is also assumed that the facility is not equipped with any attack detection scheme. The attacked signals are applied to the PtG unit, and the impact of the PtG unit operation on the transmission lines capacity is depicted in Figure 5.8. As shown in the figure, many transmission lines are overloaded with up to 30% of their nominal ratings.

For example, the main transmission line from bus 1 to bus 2 has a 15% probability to be overloaded with less than 5% of its nominal capacity; a 20% probability to be overloaded in the range between 5% to 10% of its nominal capacity; and a 5% probability to be overloaded in the range between 10% to 30%.

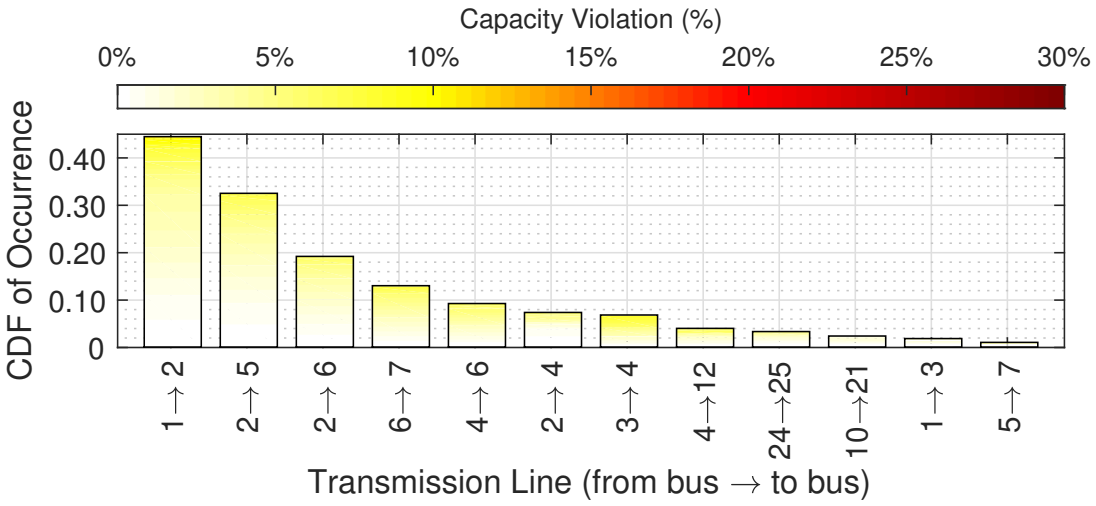


Figure 5.8: Transmission lines capacity violations during aggressive cyber–attacks without the utilization of a verification model.

5.4.3 Secondary Signals Attacks Detection

The attack detection module for the secondary signals is deployed at the PtG/GfG unit location, where it receives both the secondary and primary signals to verify the former. In this study, the PtG/GfG operating data for one year are analyzed and the operation percentage is reported in Table 5.2 for the three operating modes described in Section 5.3.2. As given in the table, PtG and GfG units are idle (i.e., zero setpoints) during 44.8% and 65.2% of the year, respectively. Conversely, the facilities operate at their rated capacity (i.e., maximum setpoints) for 41.2% and 20.2% of the year. During the remaining time, the facilities operate around 14% of the time in the range between zero and maximum. Considering such uneven three-mode operation behavior, the accuracy of secondary signal estimation can be enhanced by utilizing the proposed hybrid (C+RegNN) model. Accordingly, in the first step, the three-class classifier (ClassNN) predicts the mode of operation prior to estimating the operation setpoints. In the second step, the predicted mode is fed into the regression neural network model (RegNN) to estimate the secondary operating signal.

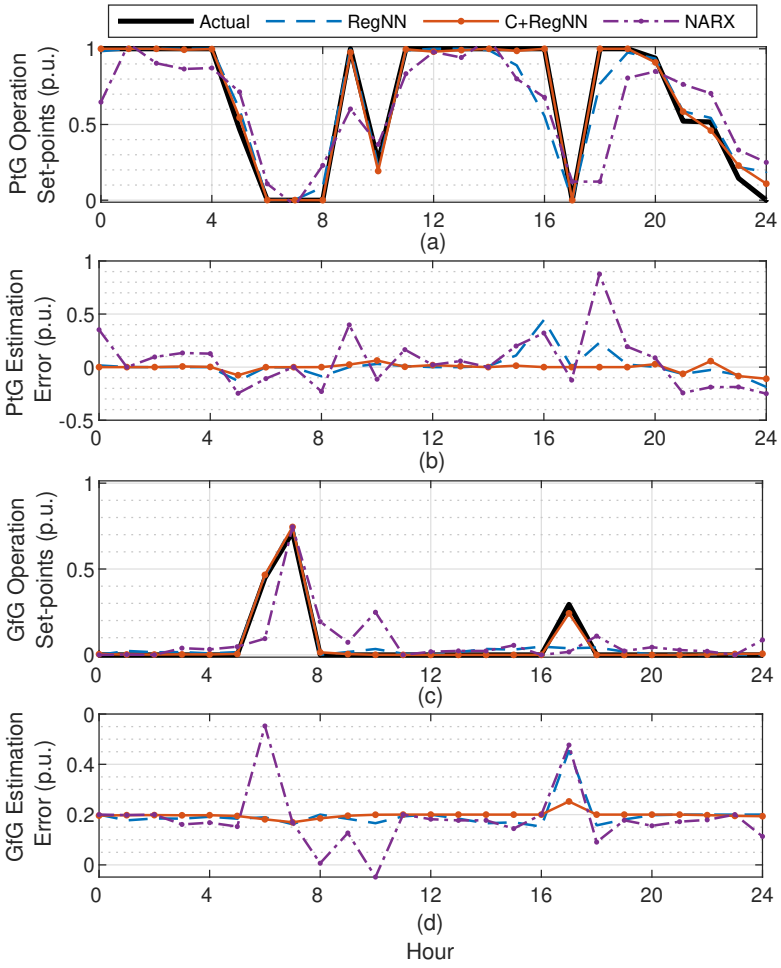


Figure 5.9: Actual and estimated operation of (a) PtG and (c) GfG units using the proposed C+RegNN compared with RegNN and NARX models; Error in estimation is compared in (b) for PtG and (d) for GfG units.

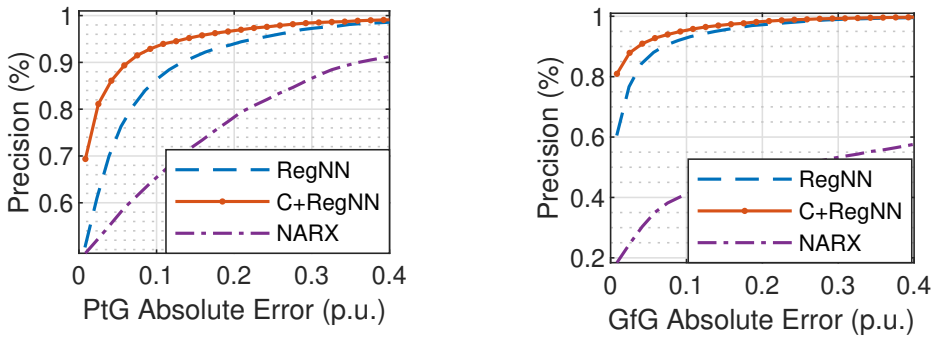
Table 5.2: Probability Distribution of Operation Mode Classes

	Zero	**In-between**	**Maximum**
PtG Facility	44.8%	14.0%	41.2%
GfG Facility	65.2%	14.6%	20.2%

To evaluate the performance of the proposed C+RegNN model, the actual signal along with the estimated one are contrasted over the entire simulation period, and the estimation error is calculated. Moreover, for comparison purposes, two additional models including the regular regression neural network (RegNN) and the Nonlinear Auto-Regressive model with eXogenous input (NARX) [159] are also presented. A daily snapshot is, then, given in Figure 5.9 (a)–(d) for detailed observations. Considering one year of operational data, the mean absolute errors are found to be 5% and 3% for the PtG operation and 3% and 1.8% for the GfG operation under the RegNN and C+RegNN models, respectively. This indicates that the proposed model is superior in performance to the typical model.

The difference between the secondary signal value received by the PtG/GfG unit and the estimated value using the C+RegNN model is reported as the estimation error. If the estimated error is below a pre-defined threshold, the signal is considered valid; otherwise, it is anomalous. Therefore, having an accurate estimation of the secondary signal is imperative to set the detection threshold to the lowest possible value.

Moreover, based on the precision curves represented in Figs. 5.10 (a) and (b), the appropriate threshold can be set to allow the legitimate signal to pass and, at the same time, block the attacked signals. As can be inferred from the curves, a threshold of 0.1 (p.u.) absolute error would allow the detection of false signals with a confidence rate of 92% and 95% for PtG and GfG units, respectively. The verification model is, then, utilized with these thresholds to clear the capacity violation issue as depicted in Figure 5.8. The results indicate that there would be no capacity violation once the verification



(a) **(b)**

Figure 5.10: Precision percentage versus absolute estimation error of (a) PtG and (b) GfG, unit setpoints using RegNN and C+RegNN models.

model is applied since the attacked signals are blocked using the proposed verification model.

5.4.4 Primary Signals Attacks Detection

In this study, the performance of the proposed mechanism for detecting the FDIA on the primary data is evaluated. Particularly, the impact of attacks on electricity prices and PV signals is assessed considering that an attacker compromises the data at different times. The performance of the proposed CNN-based detection scheme has been compared with other machine-learning-based detection schemes including Artificial Neural Network (ANN) and Support Vector Machine (SVM). The ANN is chosen as the supervised feed-forward classifier with one hidden layer of 50 neurons, whereas both the supervised two-class and unsupervised one-class SVMs schemes are implemented with the quadratic kernel. To avoid overfitting, a 5-fold cross-validation approach is implemented during the training, and the same number of labeled data for all the supervised methods is used. A different set of compromised labeled data is used for testing the three supervised detection schemes, whereas only normal data are used for training the unsupervised SVM; then, both the normal and compromised datasets are used for testing it.

FDIA scenarios are modeled assuming the adversary carefully replaces the original

Table 5.3: Results from Comparing the Accuracy of the Proposed Scheme on Detecting the FDIA on Primary Signals with Prior Machine-Learning Schemes.

Detection Method	Actual Label	Number of Testing Data	Identified as Attacked	Identified as Normal	Detection Accuracy (%)
Proposed Method	Attacked	1247	1178	69	94.47
	Normal	1247	32	1215	97.43
ANN	Attacked	1247	1124	123	90.14
	Normal	1247	57	1190	95.43
Two-Class SVM	Attacked	1247	1159	88	92.94
	Normal	1247	44	1203	96.47
One-Class SVM	Attacked	1247	783	464	62.79
	Normal	1247	76	1171	93.91

signals with the values that will pass the basic BDD filters, e.g., the adversary only modifies PV generation quantities during daytime hours. The performance of attack detection on the normal data is evaluated using the *accuracy* measure. In this work, the detection accuracy for the normal data is defined as the ratio of scenarios correctly identified as normal over the total number of normal data scenarios; whereas, the accuracy of attacked data represents the ratio of scenarios correctly identified as deceptive over the total deceptive data scenarios. Ideally, a perfect detector will have an accuracy of 100% for both normal and attack data.

The results reported in Table 5.3 indicate a comparison of the average accuracy of

Table 5.4: Accuracy of Detecting FDIA at Different Number of Attacked Samples and Training Data With/Without Noise.

Primary Signal	**Training Data**	**Attack Detection Accuracy**		
		One Sample	**Two Samples**	**Three Samples**
Electricity Price	Without Noise	87.47%	97.36%	98.56%
	With Noise	85.00%	94.80%	96.10%
PV Generation	Without Noise	91.81%	94.95%	96.39%
	With Noise	89.50%	92.80%	94.20%

the proposed CNN-based detection scheme with the ANN-based and SVM-based models. It can be observed that the proposed method achieves an average detection accuracy of 95.95% (i.e., 97.43% and 94.47% for detecting normal and attacked data, respectively), which is the highest among other models. Notably, the one-class SVM-based detector did not perform strongly in identifying the attacked data; hence, it would be superior to employ a two-class detection model with labeled training data to improve the detection accuracy.

In addition, the performance of the proposed CNN-based detector is evaluated for a variable attack window ranging from 1 to 3 data samples and considering noisy training data. The results as given in Table 5.4 represent the detection accuracy for attacks on electricity price and PV generation signals. As reported in the table, the higher the number of compromised data samples, the higher the possibility of detection will be. For instance, when noise-free training data is used, the detection accuracy increases from 87.47% at a one-sample attack to 97.36% at a two-sample attack on the electricity price

signal. Hence, the attacker cannot perform a long-standing attack without increasing the chance of being detected. Table 5.4 indicates as well that the attack detection accuracy slightly decreases when noisy data is used for training. For instance, the accuracy for detecting the attacks on the electricity price signal decreases from 87.5% to 85% when the training data is noisy under a one-sample attack. For the attacks on two and three samples, however, the accuracy decreases from 97.4% to 94.8% and from 98.6% to 96.1%, respectively. A similar trend is observed for attacks on the PV generation signal. These results indicate that the utilization of noisy synthetic data causes a negligible effect on the accuracy of the model.

5.5 Summary and Discussion

A new model is presented in this chapter for joint scheduling of PtG and GfG facilities in an integrated power and gas transmission grid that is resilient to cyber–attacks. The model utilizes the gas grid to expand the capacity of the power grid in a cyber–attack resilient framework. The operation of the integrated system during cyber–attacks, which are not detected using traditional methods, has been investigated. Using deterministic estimation, wavelet transform, and supervised and unsupervised machine-learning-based models, new schemes are developed for the verification of input and output scheduling signals in order to detect and block hacked signals. The efficacy and feasibility of the proposed model are evaluated through numerical studies and test systems. It is demonstrated that incorporation of the proposed detection models into the scheduling algorithm would create a cyber–attack resilient model in an integrated power and gas transmission grid. It is also indicated that the utilization of noisy synthetic data for model training causes a negligible effect on the accuracy of the model.

Chapter 6

Real-Time Detection of Surreptitious IoT-Based Cyber–attacks in Power Distribution Systems

6.1 Introduction

This chapter focuses on threats to Power Distribution Systems (PDSs) stemming from residential Internet of Things (IoT)-enabled appliances. Customers deploy IoT-enabled appliances to have a better quality of life and provide energy-efficient solutions making them essential components in the development of modern smart homes and cities. Despite its advantages, IoT technology poses new privacy and security challenges as they relate to the authenticity and integrity of the data gathered and exchanged by IoT devices. Such challenges can make both smart homes and PDSs vulnerable to security attacks, thereby impacting their efficiency and reliability. Therefore, it is essential to identify the security risks associated with behind-the-meter (BTM) IoT-enabled appliances to develop countermeasures to protect the PDSs. As such, a stealthy-based attack model is presented that targets a set of compromised IoT-enabled appliances to worsen the performance of these individual appliances as well as the PDS while minimizing the chance of its detection

via maintaining the operating conditions of such appliances within the comfort levels of the end-users. To counter the applied stealthy attack, a novel real-time anomaly detection and prediction method is proposed based on demand power spectrum analysis and Long Short-Term Memory (LSTM) neural networks. Further, a Feeder Loading Abnormal Power Spectrum (FLAPS) index is introduced and utilized to estimate the attack onset time, which is then reported to the PDS's operator for further investigation and action. The performance of the stealthy attack model and the proposed anomaly prediction approach are evaluated on a residential community modeled using the IEEE-13 bus unbalanced power distribution feeder, which involves a variety of power consumption patterns and appliance operation schedules. The impact of the proposed stealthy attack on the PDS is quantitatively analyzed considering the voltage violation cases and the wear and tear of the substation voltage regulators. The analysis and impact of several attack scenarios are presented.

Also, the simulation results demonstrate the superiority of the proposed technique to detect and alert for stealthy attacks in a timely manner, thereby enabling the system to operate reliably and securely.

6.2 Problem Description

The deployment of IoT-enabled appliances is scaling up as a contemporary solution for consumers to optimize energy use and leverage their comfort. Using this technology, consumers can remotely monitor and control their appliances' operation. However, the incremental installation of cyber-connected devices paves the road for adversarial remote exploitation of large amounts of electrical loads placing PDSs at risk of cyber–attacks. For instance, wireless network protocols and equipment are vulnerable to cyber–attacks that can break into the connected devices and diffuse a corrupted piece of software providing the attackers with unlimited capabilities to control the device. A limited number of technologies (such as Bluetooth) have security mechanisms that can be exploited by an

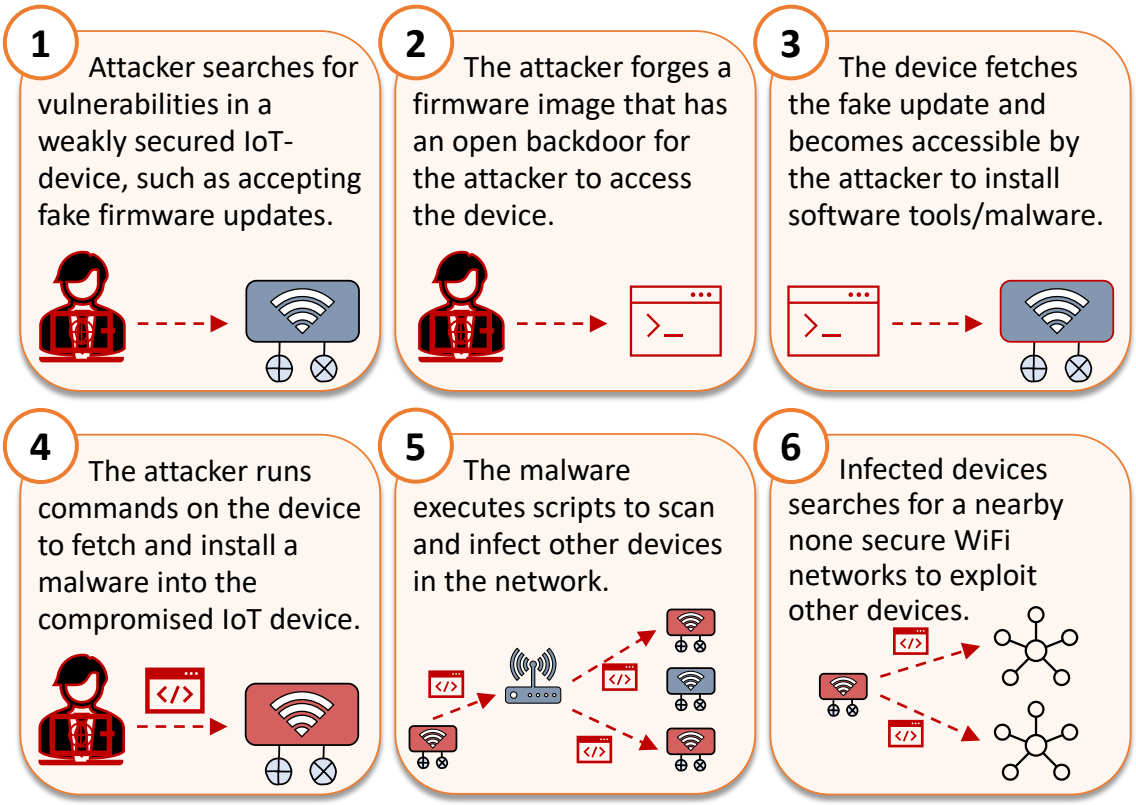


Figure 6.1: Flowchart: a potential scenario to compromise set of IoT-devices.

attacker within close proximity. These attacks are particularly destructive when multiple devices are within a receiving/transmitting range of the medium. Furthermore, certain designs, such as cloud management solutions, can act as desirable entry points for malicious software updates (for example, when their interfaces are hard-coded or weakly enforced) as illustrated in Figure 6.1. Below, we examine a few IoT devices vulnerabilities:

Communication-based: Due to the absence of established security requirements in most IoT device manufacturing markets, the existing security of IoT devices is only expected to match basic security practices. Since protecting the connection is important, the security mechanisms can have a huge impact on the possibility of an attacker compromising the device. Furthermore, communication between IoT devices and the cloud-based aggregator allows for continuous monitoring and scheduling of daily activities. It is often possible for unauthorized parties to abuse administrator-level permissions, which occur as a result of

weak aggregator-vendor interfaces. Additionally, IoT manufacturers provide their users with the capability of remotely managing their assets, including firmware updates and configuration management tools. However, these tools can also be misused if the security mechanisms are not sufficiently protected.

Deployment Factors: There might be a tangible advantage to physical proximity in determining worm/virus spreading characteristics in the future. Although most viruses are driven by the CPU of the host, recent articles suggest that malware could also exploit network controllers (i.e., WiFi) to launch attacks. The deployment level is another factor in which IoT devices can differ in their computing capabilities and software maturity. Some IoT devices come with both wired and wireless connectivity. Hence, their communication capabilities within a region will directly influence the risk of controlling a large amount of IoT-enabled appliances. The share of IoT devices by a specific manufacturer increases the risk that a large number of IoT devices can be exploited by a single attacker since all the devices share a common vulnerability. With regards to the software, IoT devices are typically updated within a few years, whereas the service life of an IoT device may exceed the designated number of years. As attacks are enhanced and devices grow older, this situation may lead to an eventual proliferation of insecure devices.

6.3 Stealthy Attack Modeling and Mathematical Formulation

This section describes the stealthy attack model on PDSs performed by an intelligent attacker utilizing a set of compromised IoT-enabled appliances. The attacker targets to maximize the damage on PDSs while considering trade-offs to minimize the cost of utilizing the limited adversarial resources and minimizing the risk of being easily detected.

Table 6.1: Adversary Model Characteristics

Resources	Class-II: Have sufficient resources to perform the attack without being easily detected.
Access	Non-possession: Physical access to compromised devices is not required.
Knowledge	Limited-knowledge: PDS's network topology and real-time compromised devices status.
Specificity	Targeted: The operation level of the compromised appliances is carefully adjusted.

6.3.1 Adversary and Attack Characteristics

It is assumed that an intelligent attacker has sufficient resources required to compromise a set of IoT-enabled appliances deployed BTM and can remotely communicate with them. In such a case, the attacker has access to real-time information of the compromised devices, i.e., can read their status besides issuing commands to change their operation setpoints. According to the classification presented in [160] and summarized in Table 6.1, this level of resourcefulness would belong to *Class-II* adversary, where it is difficult to simultaneously coordinate the operation of the compromised IoT-enabled appliances across the PDS which leads to long-lasting damages.

Having the motivation and access over a large group of compromised loads, the attacker can perform a man-in-the-middle, also described as the *non-possession*, attack. Unlike the possession access scheme where the adversary needs to physically access the compromised devices, in the non-possession scheme, the attacker does not require physical access to the compromised devices.

However, to craft sophisticated attacks, the attacker is required to acquire *limited-knowledge* about the PDS network topology to estimate the interim attack impacts. This

would, in turn, enable the attacker to control/quantify the contribution of the compromised appliances towards the targeted attack on the PDS.

The adversaries will, therefore, first, identify the set of IoT-enabled appliances to be compromised and controlled during the attack and then coordinate the operation of the compromised appliances to cause progressive damages to the PDS while maintaining IoT-enabled appliances within their prescribed operation limits. Here it is noteworthy that applying a simple, i.e., *non-targeted*, attack strategy via setting all of the compromised devices to operate at the maximum power possible, for example, could potentially lead to a premature end of the attack due to: (i) Setting the compromised appliances on extreme operating conditions increases the discomfort of consumers who will be compelled to deactivate the IoT control unit to work in manual mode or completely disconnect them from the power supply when severe abnormal operation is experienced. (ii) Such a strategy may increase the power flow unbalance to an extent that triggers local protection devices such as fuses/circuit breakers, thereby isolating the compromised household from the network.

Consequently, in this work, the adversary model is considered *targeted*, i.e., the operation level of the compromised appliances is carefully adjusted. To this end, the intelligent attacker will follow a stealthy attack approach that will steadily damage the PDS while limiting the sudden disruption; this indeed minimizes the chances of detection.

The model of the attack is assumed that the adversary strategically manipulates the setpoints of a group of compromised IoT-managed loads over time to maximize the harm caused to the PDS. For such a strategy, the attack needs to be performed multiple times, i.e., repetitive, to cause an impact. This means that the adversary will frequently change the setpoints of the compromised devices at the desired levels while maintaining the reproducibility of the attack. The type of this attack falls under data integrity attacks because it affects the integrity of the system's controls by manipulating the power setpoints or status of the compromised devices. Thereby, considering the assets vulnerable to such attacks, the adversary can target any resources that are equipped with remote control

Table 6.2: Attack Model Characteristics

Frequency	Iterative: the adversary must attack multiple loads.
Reproducibility	Multiple-times: reproduced multiple times before being detected/mitigated.
Attack Type	Data Integrity: affects the integrity of the system's controls.
Asset Targeted	IoT-enabled devices or appliances (Smart AC units, lights, water pumps, water heaters, EV chargers, etc.)

capabilities such as IoT-enabled devices or appliances (Smart HVAC units, lights, water pumps, water heaters, EV chargers, etc). A detailed mathematical formulation of the attack model is presented hereunder.

6.3.2 Optimal Attack Model

Power systems utility companies operate and maintain PDSs to supply electrical power to customers via a network of radial distribution feeders. A power meter, typically, is installed at the customer's interface point with the grid, also known as the *grid edge*. After this point, the utility company is oblivious to the operation of the supplied loads, however, the aggregated energy consumption is recorded.

Considering the PDS system shown in Figure 6.2, which feeds a residential area, a realistic assumption is made that not all houses are equipped with IoT-enabled appliances. Let's assume that a cyber adversary can compromise a group of IoT-enabled appliances, denoted as $\mathcal{A}$, deployed in the houses, shown in red color. The compromise includes the ability of the adversary to monitor and update the setpoints of the appliances, thereby, controlling a portion of the electric power demand supplied by the PDS. Accordingly, in preparation to perform the attack, the adversary silently observes the operation of the

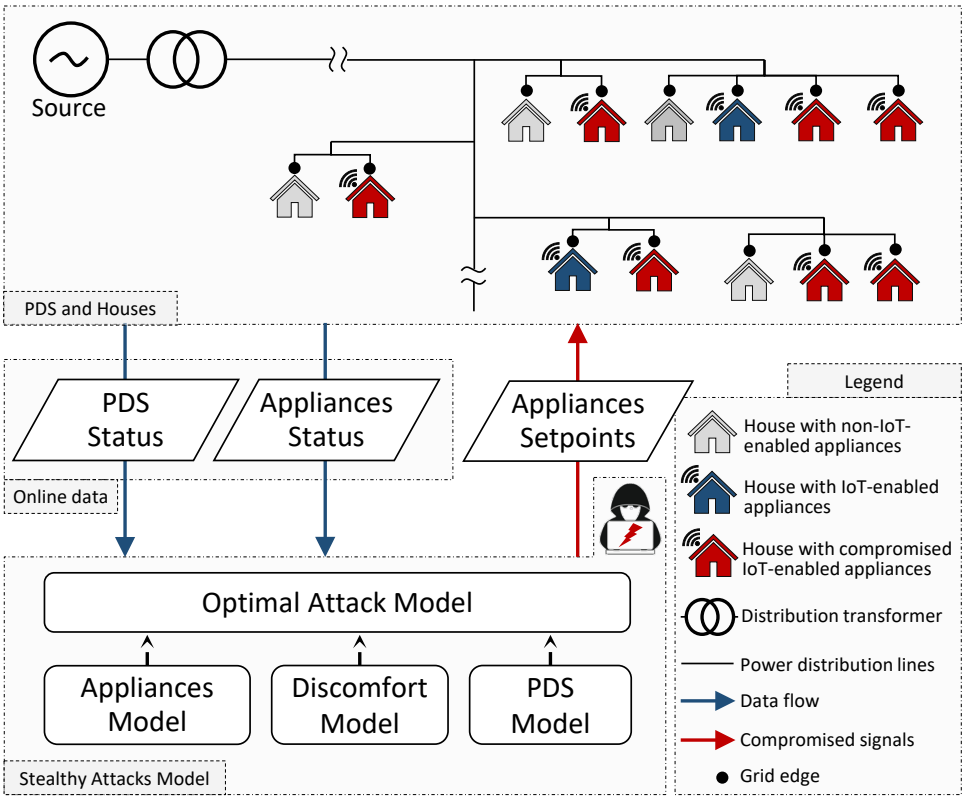


Figure 6.2: Schematic of the attack model on PDSs via compromised IoT-enabled appliances.

compromised appliances and deduces the attributes of their control scheme properties. This data is then utilized to target specific appliances to deteriorate the power quality of PDSs. The aim is to introduce maximum variations in the total power consumption with minimal impact on the discomfort to the end-users. As such, the optimal attack strategy $\mathcal{S}_A$ is formulated as follows:

$$\mathcal{S}_A : \begin{array}{ll} \max\limits_{s_a(t)} & \sum\limits_{a \in \mathcal{A}} \left[\beta_a \dfrac{\Delta P_a(t)}{P_a^{\mathrm{R}}} - \left(1 - \beta_a\right) \xi_a(t) \times \epsilon_a(t) \right] \\ \text{s.t.} & 0 \leq s_a(t) \leq 1 \end{array} \tag{6.1}$$

which is subject to the operational constraints of the compromised IoT-enabled appliances $a \in \mathcal{A}$ as will be discussed in Subsection 6.3.4. Here, the optimization variable $s_a(t)$ is linked to the appliance's power demand model. In this optimal model, the first term of the sum, to be maximized, represents the normalized power demand difference that will be induced by the adversary via manipulating the setpoints of the compromised IoT-enabled appliances. The numerator of this term, $\Delta P_a(t)$, is the power demand difference, while the denominator, P_a^{R}, is the rated power of the appliance.

On the other hand, the second term, to be minimized, of equation (6.1) denotes the discomfort levels that will be experienced by consumers after performing the attack via uploading the new settings to the compromised IoT-enabled appliances. The parameter $\beta_a \in [0, 1]$ permits the adversary to adjust the trade-off between maximizing the severity of the attack versus minimizing the consumers' discomfort which is expressed in the terms $\xi_a(t)$ and $\epsilon_a(t)$ as will be discussed in the coming subsection. By solving the problem in equation (6.1), the values of the optimization variables $s_a(t)$, are identified and then utilized by the adversary to calculate the new operation setpoints of the compromised IoT-enabled appliances.

6.3.3 Appliance Discomfort Model

While carrying out attacks via the compromised IoT-enabled appliances, the adversary manipulates their operation, thereby affecting the comfort of the end-users. This discom-

fort arises from two causes:

1. Mandating the users to experience extended waiting times for the appliance to operate or be ready, e.g., increasing EV charging time.

2. Operating the appliance at a different capacity than what is needed for the comfort of the user, e.g., setting the Air Conditioner (AC) thermostat away from the user's comfort range.

Hence, maintaining relatively low discomfort levels while performing the attack will help in lasting the stealthy attack longer and more impactful. The level of discomfort experienced by an appliance consumer can be measured based on the amount of deviation from the preferred setpoint operation settings assigned by the end-user. More formally, for a particular appliance a configured to operate at a user-preferred property setpoint $u_a(t)$, the discomfort level the end-user experiences due to appliance operation at a different level $\hat{u}_a(t)$ can be measured using the following equation:

$$\xi_a(t) = \frac{|u_a(t) - \hat{u}_a(t)|}{u_{a,\max} - u_{a,\min}} \tag{6.2}$$

where $u_{a,\max}$ and $u_{a,\min}$ are the property's maximum and minimum values. For instance, the brightness level for dimmable lights can be set between 0% and 100%, thus $u_{a,\min} = 0$ and $u_{a,\max} = 100$, while a space heater with three operation levels as 'off', 'low' and 'high' has $u_{a,\min} = 0$ and $u_{a,\max} = 2$; and for the AC unit, $u_{a,\min}$ and $u_{a,\max}$ are the minimum and maximum temperature settings of the thermostat.

Here, it is worth noting that frequent disruptions of one particular appliance are more likely to trigger the attention of end-users, hence, increasing the chances of blocking/disabling the IoT-based operation mode. For this reason, the time between attacks measure is introduced that the adversary uses to account for disruptions due to frequent manipulation of the same appliance. The introduced measure is based on the time elapsed since a particular appliance's settings have been manipulated by the adversary. The longer this elapsed time, the lesser disturbances incurred to that particular appliance. To restrict

the values of this measure in the range between $[0, 1]$, the exponential function is utilized as expressed in the following equation:

$$\epsilon_a(t) = \exp\left(\gamma^{\epsilon}(t_{a,\epsilon} - t)\right) \tag{6.3}$$

where $t_{a,\epsilon}$ (less than t) is the timestamp of the last manipulation instance or zero if the appliance has never been attacked, and γ^{ϵ} is a sensitivity factor.

6.3.4 Smart Appliances Load Model

Smart IoT-enabled appliances provide the option to automatically adapt their operation based on learning about the end-user usage patterns. This option permits operation with less direct involvement from the end-user, thereby increasing their comfort and convenience. Attackers targeting compromised IoT-enabled appliances can exploit this feature to change appliance settings without significantly impacting the comfort of the end-user. As such, accurate appliance control models are essential to quantify the attack impact on the appliance operation, hence inferring the impact on the deterioration of the PDS power quality.

The instant power consumption of an appliance $a \in \mathcal{A}$, at time t, is given in the equation (6.4) as follows:

$$P_a(t) = P_a^{\mathrm{R}} \times s_a(t) \qquad \forall a \in \mathcal{A} \wedge t \in \mathcal{T}, \tag{6.4}$$

where P_a^{R} represents the rated power of the appliance, and $s_a(t) \in [0, 1]$ is the status set by the control scheme. Broadly speaking, home appliances can be clustered into (i) thermal-based models, i.e., their operation depends on temperature sensors and thermostat settings such as AC, fridge, and water heaters; and (ii) non-thermal-based models include all other appliances such as lights, plugin electric chargers, irons, TVs, etc. Following this classification, attackers can model the compromised appliance control scheme as follows:

Thermal-based Control Scheme

Thermal-based appliances, denoted as $\mathcal{A}_{\mathrm{T}}$, are normally controlled using a hysteresis thermostat, which switches the appliance '*ON*' and '*OFF*' when the temperature of the medium (air for the AC and fridge, and water for water heaters, respectively) drops or exceeds a reference band. Formally, the status of these appliances is given in equation (6.5) as follows:

$$s_a(t) = \begin{cases} 0 \text{ ('OFF')}, & \text{if } T_a \leq T_{\text{set},a} - \delta_a^{\mathrm{T}}/2 \\ 1 \text{ ('ON')}, & \text{if } T_a \geq T_{\text{set},a} + \delta_a^{\mathrm{T}}/2 \\ s_a(t-1) & \text{otherwise} \end{cases} \quad \forall a \in \mathcal{A}_{\mathrm{T}} \wedge t \in \mathcal{T}, \tag{6.5}$$

where δ_a^{T} is the dead-band value specified by the manufacturer, and $T_{\text{set},a}$ is the reference setpoint temperature preferred by the consumer. According to the U.S. Department of Energy, the ideal home AC temperature is 68°F and 78°F (20°C and 25°C) during the winter and summer seasons, respectively [161]. For the fridge, the ideal temperature setpoint is 37°F (4°C) [162].

Using this control model, Figure 6.3 illustrates the correlation between three signals: (i) the power consumption of an AC in Figure 6.3-(a), (ii) the associated indoor temperature in Figure 6.3-(b) blue color, and (iii) the cooling setpoint value in Figure 6.3-(b) orange color. As can be noticed in the figure, the power consumption signal oscillates between zero and maximum consumption rates to maintain the indoor air temperature at the setpoint value. Additionally, changes in the setpoint do not cause an instant change in power consumption levels. Therefore, considering the hysteresis model, an attacker can better estimate the impact of manipulating the setpoint on power consumption compared to the fixed on/off model.

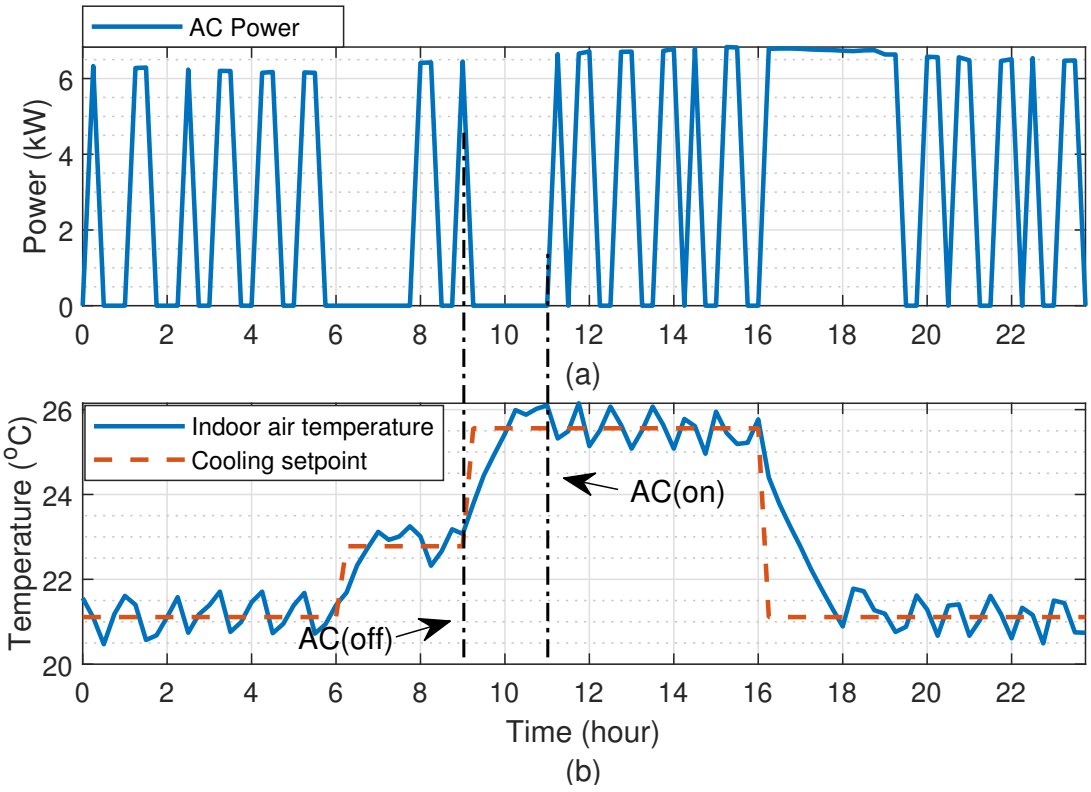


Figure 6.3: One day profile of (a) The power consumption signal of an AC, and (b) the associated indoor temperature and setpoint signals.

Non-Thermal-based Control Scheme

Appliances under this category typically operate consistently at either one of two states as 'on' or 'off'. Examples of such appliances include conventional two states lights, fans, TVs, computers, and appliances controlled using ad-hoc smart plugs. On the other hand, there are non-binary state appliances that operate at any level between zero and the maximum rating such as dimmable lights which are controlled via adjusting the brightness levels, and EV chargers where the charging speed adjusts the instant demand power.

Therefore, the control scheme of the appliances under this category can be modeled as follows:

$$s_a(t) = \frac{u_a(t)}{u_{a,\max}} \qquad \forall a \in \mathcal{A}/\mathcal{A}_{\mathrm{T}} \wedge t \in \mathcal{T}, \tag{6.6}$$

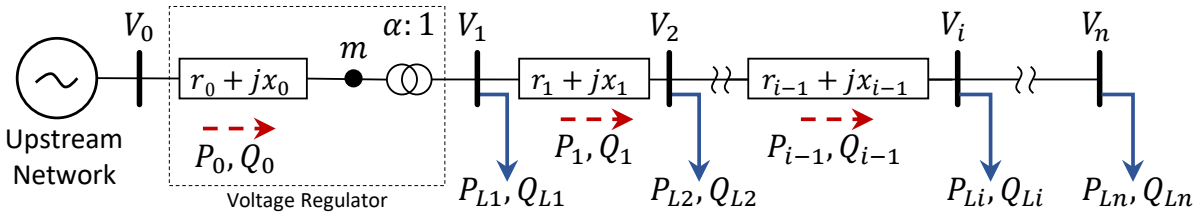


Figure 6.4: Radial feeder in a PDS.

The term in the denominator ensures that for any valid value to the property u_a, the corresponding $s_a(t)$ will be either 0 or 1 for two-state operation appliances, and within the range $[0, 1]$ for non-binary state appliances.

6.3.5 Adversary Power Distribution System Model

To estimate the power quality deterioration in a PDS due to a targeted attack, the adversary needs to have an appropriate model for the PDS. A 3-phase balanced feeder in a radial PDS is shown in Figure 6.4. In this feeder, the active P_i power flow in a specific line i; and the voltage square at bus i, $U_i = V_i^2$, can be formulated using the simplified DistFlow model [163] as follows:

$$P_i(t) = \sum_{k\,=\,i+1}^{n_{\text{br}}} \sum_{h\,\in\,\mathcal{H}_k} \sum_{a\,\in\,\mathcal{A}_h} P_{a,\,h}(t) \tag{6.7a}$$

$$U_i(t) = 1 - 2\sum_{k=1}^{i-1} \Big(r_k P_k(t) \Big) \tag{6.7b}$$

where $P_{a,\,h}(t)$ is the active power demand at time t of the appliance a which belongs to the group of appliances $\mathcal{A}_h$ inside the house $h \in \mathcal{H}_k$ where $\mathcal{H}_k$ is the group of houses connected to bus k; and r_i is the line's resistance. In this simplified mode, the reactance of the lines is assumed to be much smaller than the lines' resistance therefore can be ignored. It is also assumed that the adversary can infer the approximate locations of the compromised IoT-enabled appliances via utilizing communication network tools such as IP address to Geo-location lookup.

Now, if an adversary targets the operation of the appliance a in the house h, its active power demand will change by $\Delta P_{a,\,h}(t) = P_{a,\,h}(t) - P_{a,\,h}(t - \Delta t)$. Such change in the power demand causes a change in the branches' power flow expressed as follows:

$$\begin{aligned}\Delta P_i(t) &= P_i(t) - P_i(t - \Delta t) \\ &= \sum_{k\,=\,i+1}^{n_{\text{br}}} \sum_{h\,\in\,\mathcal{H}_k} \sum_{a\,\in\,\mathcal{A}_h} P_{a,\,h}(t) - \sum_{k\,=\,i+1}^{n_{\text{br}}} \sum_{h\,\in\,\mathcal{H}_k} \sum_{a\,\in\,\mathcal{A}_h} P_{a,\,h}(t - \Delta t) \\ &= \Delta P_{a,\,h}(t) \end{aligned} \tag{6.8}$$

Similarly, the change in the bus voltages could be estimated as follows:

$$\begin{aligned}\Delta U_i(t) &= U_i(t) - U_i(t - \Delta t) \\ &= -2\left(\Delta P_{a,\,h}(t) \sum_{k=0}^{i-1} r_k\right) \end{aligned} \tag{6.9}$$

Such sustained and frequent changes on the bus voltages will trigger voltage regulation devices such as Line Voltage Regulators (LVRs) to adjust their tap settings to maintain the voltage within the prescribed limits. Standard LVRs regulate the voltage within $\pm 10\%$ range of the nominal voltage with 32 steps, or 0.625% voltage per tap [164]. Hence, the number of tabs can be calculated as:

$$\Delta\eta(t) = \left\lfloor \tfrac{8}{5} |\Delta V_{ref}(t)| \times 100 \right\rceil \tag{6.10}$$

where the operator $\lfloor \cdot \rceil$ denotes the round operation to the nearest integer. Accordingly, maximizing the power difference across the PDS buses, maximizes the voltage change at the reference bus and forces the LVR to change the taps more frequently.

6.4 Proposed Attack Prediction and Detection Framework

This section presents the proposed proactive approach to detect anomalous patterns in the power system's feeder consumption considering stealthy adversary controlling a large number of compromised customers IoT-enabled loads.

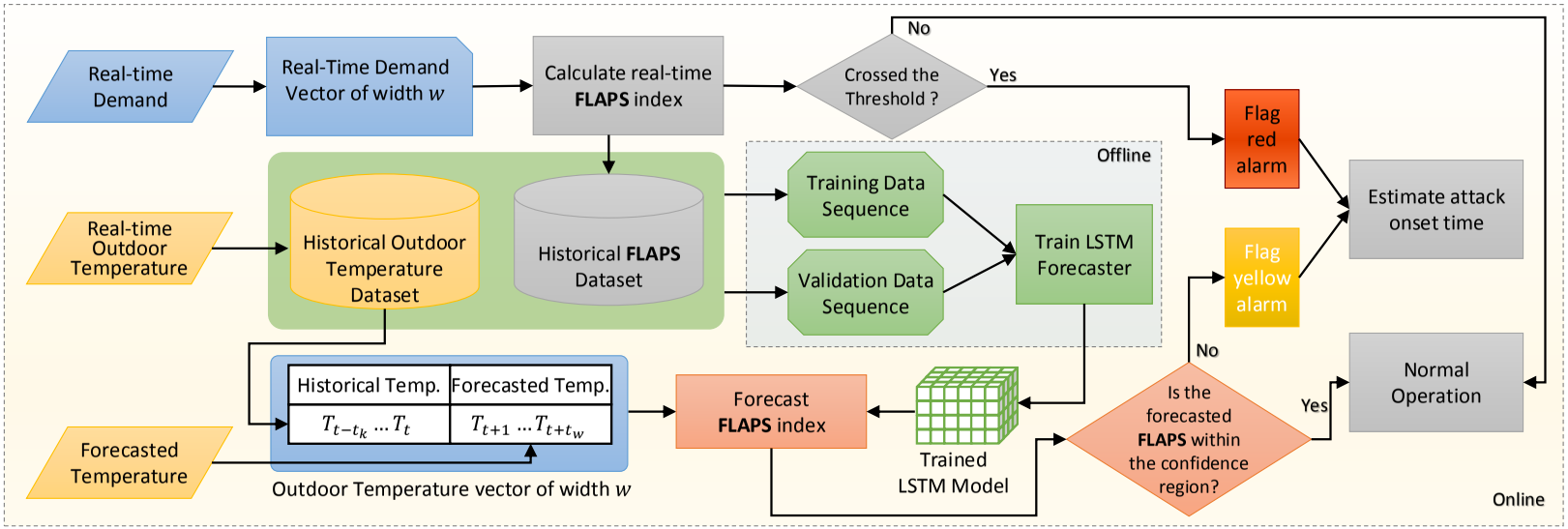


Figure 6.5: The proposed anomaly prediction and detection framework.

6.4.1 Overview of the Proposed Framework

Figure 6.5 presents a schematic diagram of the proposed framework for attack prediction and detection. First, the real-time demand data of substation feeders is collected from the local measurement points at every time step Δt. A demand vector of size w-time window is constructed, and the FLAPS index, as explained in Section 6.4.2, is calculated. Afterward, the real-time index value is compared with a predefined threshold to detect any abnormal demand behavior and is also stored in a dataset of historical FLAPS values. The aforementioned steps constitute the path for real-time anomaly detection including identification of an abnormal condition, triggering a red-flag alarm, and notifying the operator. Besides the demand data, the real-time outdoor temperature readings at the substation are collected from a local thermostat and stored in a dataset of historical temperature data. This dataset along with the FLAPS dataset are divided into training and validation sets utilized for the offline training of the LSTM anomaly prediction model. Once the model is trained and deployed, the forecast temperature for the next w-time window ahead, retrieved from a weather forecasting service, along with the historical temperature are combined and fed as an input to the FLAPS prediction model. Furthermore, the real-time FLAPS values are compared against the confidence prediction region, and a yellow flag is triggered once the values cross the confidence region boundary; then the operator is notified. After the alarms are triggered, the time at which the attack has been started is estimated. The proposed framework uses a multi-LSTM-model for accurate multi-step FLAPS prediction. The details of the proposed method are presented in the following subsections.

6.4.2 Feeder Loading Abnormal Power Spectrum (FLAPS) Index

A typical PDS monitors the real-time operating status of the power distribution feeders and collects information about various signals such as voltage and power consumption.

For the safe operation of the PDS, basic protection schemes are normally deployed and activated whenever any of the system states deviate outside the standard operating limits. To avoid being easily detected, an intelligent adversary will choose to perform hidden stealthy attacks that do not cause any violation in the system states; hence it would not trigger standard protection schemes. However, due to their incremental nature, in the long run, stealthy attacks can still instigate damage to the PDS equipment and deteriorate the power quality.

As such, the proposed detection scheme relies on observing real-time active power flow patterns of distribution feeders and comparing them with historical patterns to decide the onset of the attack. It is valid to assume that measurements collected inside the PDS substations are secure against cyber–attacks given the amount of investment modern power utilities have spent to defend their critical infrastructure. It is worthy to mention that the proposed scheme can be easily deployed in existing PDS digital metering systems and does not require the deployment of remote advanced meters since no external demand signals are involved.

Considering a PDS equipped with a real-time power monitoring system that collects and stores the aggregated feeder's power demand at every time interval Δt. At any time t, we denote the aggregated feeder's active power as $P(t)$ which is retrieved from the power meter installed at the distribution substation. At a time t_0, the active power demand signal for a time-span T is formulated as:

$$\mathbf{P}_{t_0} = [P(t_0 - T), ..., P(t_0 - \Delta t), P(t_0)] \tag{6.11}$$

The demand signal is then filtered to remove the deterministic trends. This process involves removing the effects of trends from the signal to focus on the differences in values from the trend, i.e., to identify periodic components in the power demand signal. The trend in the signal can be modeled as the polynomial $F_m(t) = \sum_{i=0}^{m} a_i t^i$ of degree m and coefficients a_i. The value of the coefficients is calculated using the least square method.

The power demand signal after removing the trend $\hat{\mathbf{P}}_{t_0,m}$ is defined as follows:

$$\hat{\mathbf{P}}_{t_0,m}(t) = \mathbf{P}_{t_0}(t) - F_m(t) \qquad \forall t \in [t_0 - T, t_0], \tag{6.12}$$

the error in the signal $\hat{\mathbf{P}}_{t_0,m}$ is calculated using the Mean Absolute Error (MAE) value as:

$$\zeta_{t_0,m} = \frac{1}{T} \sum_{t=t_0-T}^{t0} \left| \hat{\mathbf{P}}_{t_0}(t) \right| \tag{6.13}$$

The trend with the minimum error can remove most of the deterministic components from the signal; hence, the degree of the polynomial is increased until the error is less than the predefined threshold, i.e., $\zeta_{t_0,m} \leq \zeta_{min}$, or the trend reached the maximum polynomial degree $m \leq m_{max}$.

Next, the detrended signal is modeled using the Fourier transform to extract the exponential coefficients $c_{t_0,n}$, as described in the following equation:

$$\hat{\mathbf{P}}_{t_0}(t) = \sum_{n=0}^{N} c_{t_0,n} \exp\left(j2\pi n f_s t\right) \ , \tag{6.14}$$

where f_s is the sampling frequency of the demand signal, and N is the order of the harmonics. The Feeder Loading Abnormal Power Spectrum (FLAPS) index, denoted as Γ, at time t_0 is introduced as follows:

$$\Gamma_{t_0} = \frac{20 f_s}{f_H - f_L} \sum_{t=t_0-\tau}^{t_0} \sum_{f_n=f_L}^{f_H} \log_{10}\left(c_{t,n}\right) \tag{6.15}$$

where $\tau = \mu \Delta t$ is the period during which the index Γ_{t_0} is smoothed to become less sensitive to instantaneous demand variations.

Detecting abnormal feeder demand conditions is done by comparing the Γ_{t_0} index against a threshold calculated from the historical demand readings of the feeder, collected over a period of time of the year $\mathbb{T}$ as follows:

$$\Gamma_{max} = \gamma \max_{t \in \mathbb{T}} \{\Gamma_t\} \tag{6.16}$$

where $\gamma \geq 1$ is a marginal factor adjusted to control the detection sensitivity. Finally, the complete steps for computing the Γ_{t_0} index and attack detection are shown in Figure 6.6.

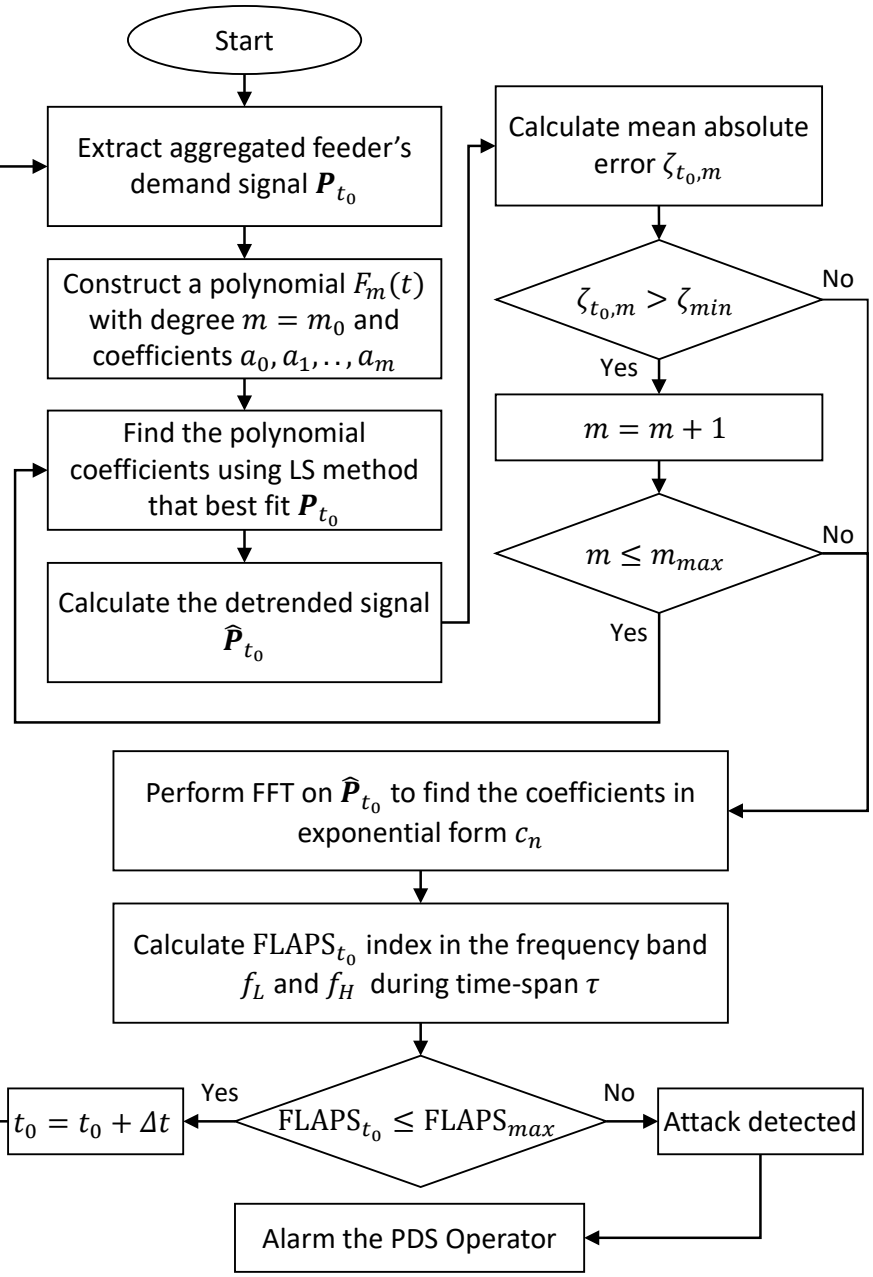


Figure 6.6: Flowchart of the steps to calculate the proposed FLAPS index.

6.4.3 Anomaly Detection via FLAPS Prediction

During low-profile stealthy attacks, the adversary attempts to introduce small perturbations in each time step; hence, the aggregated momentary impact on the distribution feeder may not be significant to immediately activate the real-time FLAPS detection mechanism described in the previous section. As such, while the incremental deviation in the FLAPS index falls below the detection threshold, the attack is unnoticed, and the adversary would be able to compromise the system parameters. The mean time between the onset of the attack and the point at which it is discovered is also known as the Mean Time to Detection (MTTD) [165]. Therefore, the prediction-based anomaly detection approach is proposed that significantly reduces the MTTD by developing a FLAPS index prediction model to predict the index values during the future time-span. Once the real-time values diverge beyond the expected prediction error levels, an alarm is triggered to notify the operator for close inspection and investigation. The model is developed using multi-models of LSTM neural network for accurate multi-step prediction.

LSTM Architecture

The LSTM neural network addresses the issue of vanished gradients seen in its predecessor Recurrent Neural Network (RNN) [166]. Using the recent input vector, the LSTM neural network would be able to model the variable temporal behavior of a time-series data set by updating the information stored in the LSTM cells' internal structure and transferring data to the connected cells, as shown in Figure 6.7. The output of the three gates in the internal LSTM structure: the input i_t, the forget f_t, and the output O_t; are controlled with the sigmoid function σ which produces values between 0 and 1. At a time-step t, x_t represents the input to the LSTM cell, (C_{t-1}, C_t) and (h_{t-1}, h_t) are the cell states and hidden states at time-steps $t-1$, t, respectively. The equations that govern the values of

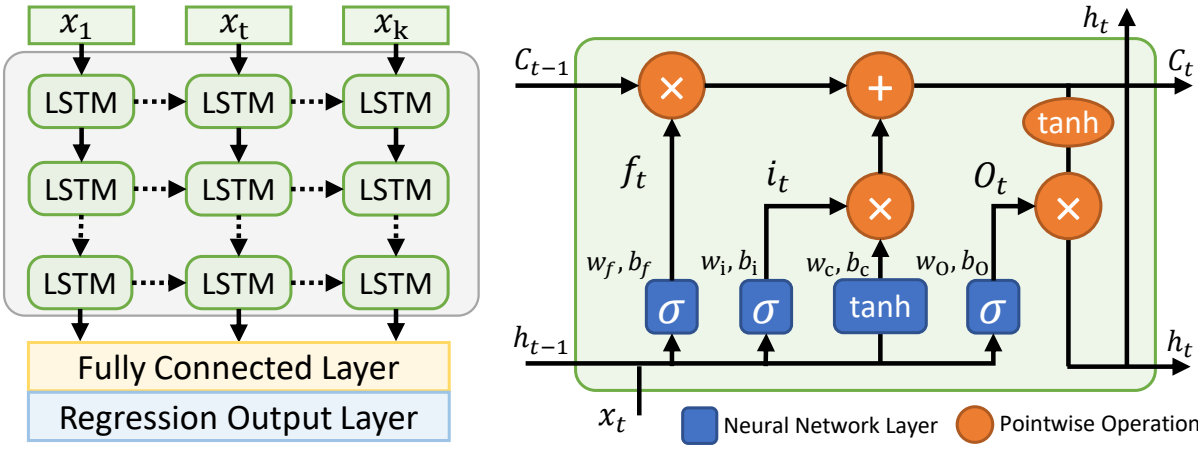


Figure 6.7: Left: the unfolded LSTM neural network model structure consists of inter-linked LSTM cells in the hidden layers; Right: LSTM cell's inner structure.

this LSTM internal structure are described as follows:

$$c_t = \tanh(W_c x_t + U_c h_{t-1} + b_c) \tag{6.17a}$$

$$i_t = \sigma(W_i x_t + U_i h_{t-1} + b_i) \tag{6.17b}$$

$$f_t = \sigma(W_f x_t + U_f h_{t-1} + b_f) \tag{6.17c}$$

$$o_t = \sigma(W_o x_t + U_o h_{t-1} + b_o) \tag{6.17d}$$

$$C_t = c_t \odot i_t + C_{t-1} \odot f_t \tag{6.17e}$$

$$h_t = \tanh(C_t) \odot o_t \tag{6.17f}$$

where W and U represent the weight matrices, and b is the bias vector. C_t and h_t represent the memory state and the output of the LSTM cell at the time-step t. The operation $\odot$ is the element-wise product of two matrices.

Data Pre-processing and Normalization

To formulate the target variable of the prediction model, FLAPS values are retrieved from the corresponding dataset and represented as a time-series sequence $\mathbf{\Gamma} = [\Gamma^{(1)}, ..., \Gamma^{(N)}]$. The input data is formulated using the covariates variables recorded at the corresponding time-step that the FLAPS index is calculated. $X = [\mathbf{x}^{(1)}, ..., \mathbf{x}^{(N)}]$ where each $\mathbf{x}^{(t)} =$

$[x_1^{(t)}, ..., x_m^{(t)}]$ is of m-dimensional vector and m represents the number of features. Without loss of generality, in the proposed model, a one-feature vector of historical outdoor temperature values is utilized as the covariate. It is common to utilize temperature for demand forecasting applications [167], however, other meteorological or calendar variables can also be considered for the prediction task. Furthermore, to improve the performance of the model, the target and input variables are normalized in the range of [0, 1] using the min-max normalization approach, as follows:

$$\hat{x} = \frac{x - x_{min}}{x_{max} - x_{min}} \tag{6.18}$$

where $\hat{x}$ is the normalized value, and x_{min} and x_{max} are, respectively, the minimum and maximum values extracted from the training dataset and utilized for the new data during the forecast process.

The Prediction Model

The prediction model utilizes data from the previous time points as a reference to estimate the next time points. Predicting a single future time point is known as the one-step forecast implemented by moving a sliding regression window one step at a time. That is for a sliding window with the size of T time points, the combined input/target vector at time t is $[\mathbf{x}^{(t-T)}, ..., \mathbf{x}^{(t)}, \Gamma^{(t)}]$. However, considering the stealthy attack model discussed in Section 6.3, the incremental changes in the demand will corrupt the recent real-time measurements of the FLAPS index; hence, it misleads the prediction model by providing corrupted data into producing anomalous predictions, i.e., the values of the index will fall within the tolerated error. Therefore, it is required to adopt a multi-step ahead prediction approach with a future time horizon of size w-time-steps that utilizes the historical data that has not been corrupted.

A simple method to predict the next w time-series values can be achieved by recursively utilizing the predicted one-step value at the current time t as an input to the model; then, predicting the next value at time $t + 1$, and so on as illustrated in Figure 6.8-(A).

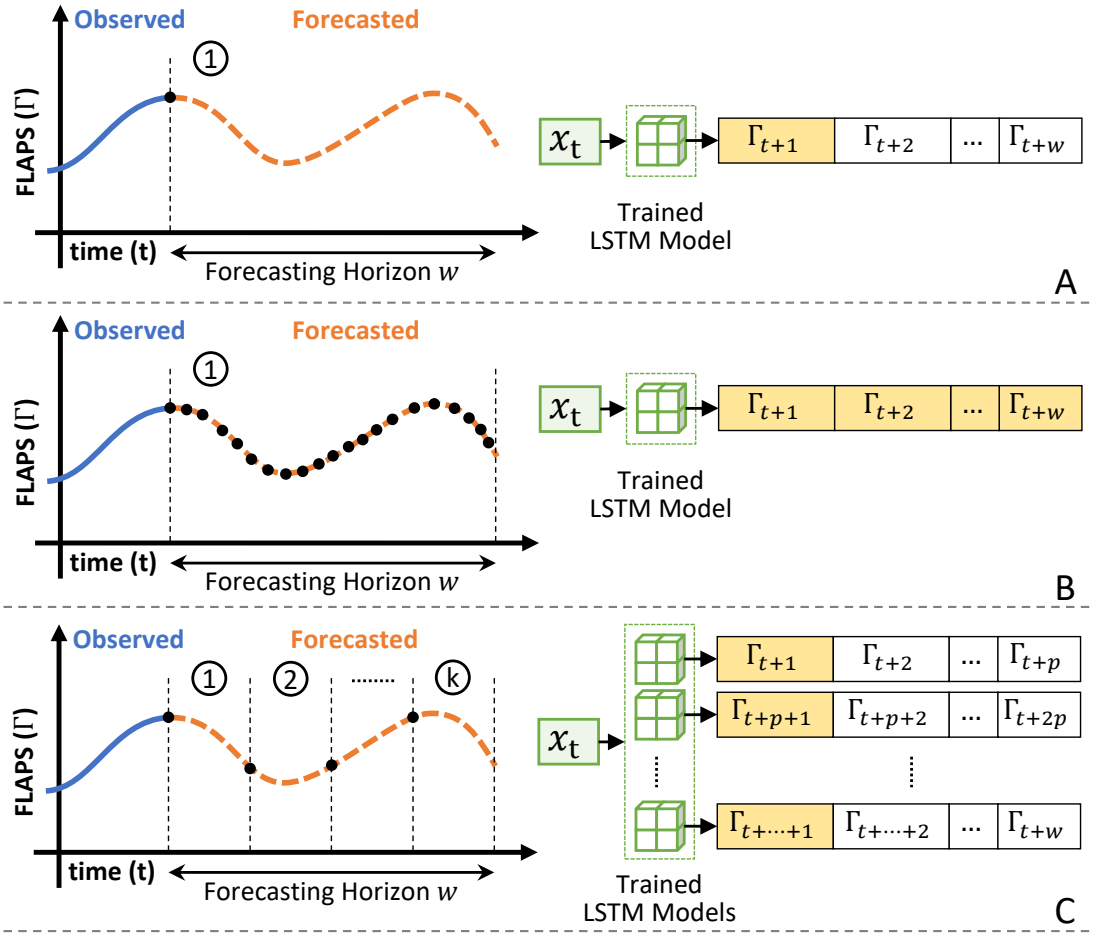


Figure 6.8: Three multi-step prediction approaches: (A) single-model recursive one-step, (B) multi-model recursive one-step, and (C) single-model multi-steps.

However, the accuracy of such an approach degrades while moving away from the initial time step. In contrast, the multi-step time series forecast, Figure 6.8-(B), can be achieved by fitting an individual model to each future time step of the prediction horizon, i.e., training w models. Although this approach may improve prediction accuracy, training and maintaining multiple models require extensive computing resources. Therefore, a hybrid approach is proposed, where a number of models k is selected to predict the future p-step of the target variable; i.e., the prediction time horizon is divided into k-period and the time points in each period are predicted using the individual one-step forward model,

as illustrated in Figure 6.8-(C).

Prediction Accuracy Evaluation Criteria

The error in FLAPS index value prediction is calculated by finding MAE which is the difference between the observed actual value and the predicted value of the index at time t, as follows:

$$e_t = \Gamma_t^{obs} - \Gamma_t^{prd} \tag{6.19}$$

$$\text{MAE} = \frac{1}{N-w} \cdot \sum_{t=w+1}^{N} |e_t| \tag{6.20}$$

The overall prediction accuracy of the model is evaluated using the Mean Absolute Percentage Error (MAPE) which is commonly utilized to evaluate prediction models [168]. MAPE is calculated as follows:

$$\text{MAPE} = \frac{1}{N-w} \cdot \sum_{t=w+1}^{N} \left| \frac{\Gamma_t^{obs} - \Gamma_t^{prd}}{\Gamma_t^{obs}} \right| \times 100 \tag{6.21}$$

where Γ_t^{obs} and Γ_t^{prd} are, respectively, the observed actual value and the predicted value of the FLAPS index at time t.

Anomaly Detection and the Confidence Region

During the validation and testing phases, the forecast from the prediction model is used to compute the error at each point in the observed data. The error value e_t at each point $t \in [1+iw, (i+1)w] \forall i \in [0, n] \wedge n = (N-w)/w$ is computed (n is the number of times of the prediction at point t); therefore, the error vector is formulated as:

$$\mathbf{e} = \begin{bmatrix} e_1 & e_2 & \dots & e_w \\ e_{1+w} & e_{2+w} & \dots & e_{2w} \\ \vdots & \vdots & \vdots & \vdots \\ e_{1+(n-1)w} & e_{2+(n-1)w} & \dots & e_{nw} \end{bmatrix},$$

which can be written as: $\mathbf{e} = [\mathbf{e}^{(1)}, ..., \mathbf{e}^{(w)}]$ where each $\mathbf{e}^{(i)}$ represents the prediction error vector at the time point $i \in [1, w]$. Then, the error vectors are modeled to fit multivariate Gaussian distribution $\Theta = \mathcal{N}(\mu_i, \sigma_i)$. For an error vector $\mathbf{e}^{(i)}$, its likelihood $\hat{p}_i$ is calculated using the distribution Θ at point i. As such, the Maximum Likelihood Estimation (MLE) approach is applied on the test errors calculated from the testing dataset to estimate the values for μ_i and σ_i. Using the MLE estimates and for a confidence level of $(1-\alpha)\%$, the confidence interval bounds $[C_i^-, C_i^+]$ for the prediction at point i are calculated as [169]:

$$\begin{aligned} C_i^+ &= \hat{p}_i + z_{\alpha/2}\sqrt{\hat{p}_i(1-\hat{p}_i)/n} \\ C_i^- &= \hat{p}_i - z_{\alpha/2}\sqrt{\hat{p}_i(1-\hat{p}_i)/n} \end{aligned} \tag{6.22}$$

where z_c is the $(1-c)$ quantile of the standard normal distribution. During the real-time operation, an observed value of the FLAPS index Γ_t is reported as 'anomalous' if the likelihood estimate $\hat{p}_{i_t}$ of the calculated error in equation (6.19) falls outside the confidence interval $[C_i^-, C_i^+]$. The confidence region of the prediction is confined between the two curves C_i^- and C_i^+ $\forall i \in [1, w]$.

6.5 Case Studies and Discussion

The performance of the developed attack and detection method is evaluated via simulations conducted on a modified IEEE-13 Bus system modeled in GridLab-D power system simulator [170], while the analysis is performed on MATLAB. The LVR is configured to regulate the voltage at bus-671 with 60V bandwidth and 30 sec. time delay. The impacts on the feeder's daily load curve, the power demand of a set of houses, and bus voltage during several attack scenarios are presented. The simulation time-step is set to -minute and the aggregated power demand of the community of 934 houses is collected at a 1-sample per 15 minutes rate.

It is expected that during adverse attack conditions, system protection devices will operate to protect the system against under/over voltage surges, thereby, causing a power

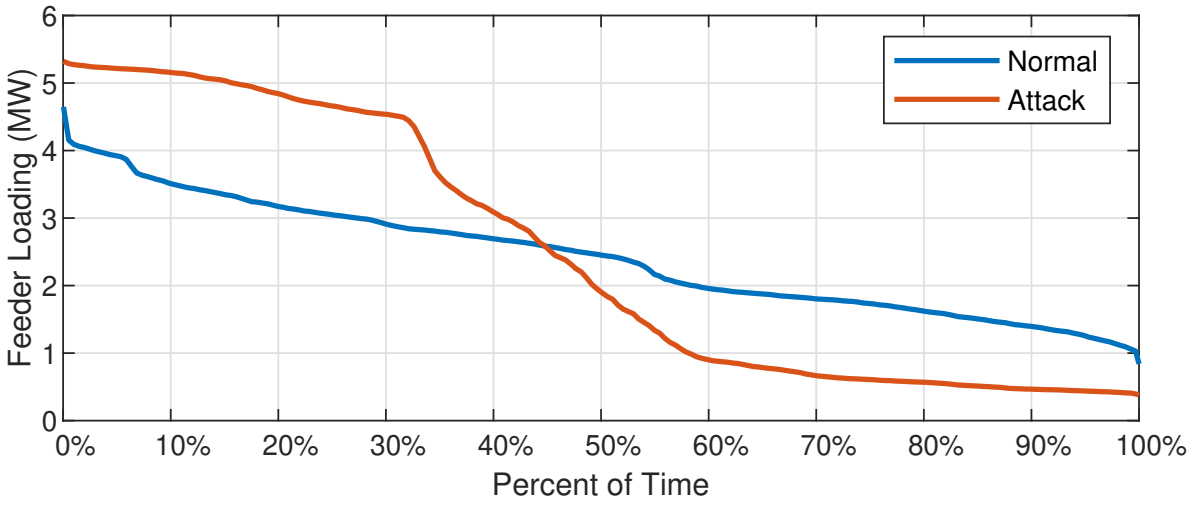


Figure 6.9: Feeder's load duration curve during normal and attack scenarios.

shutdown. Nonetheless, during less severe attack scenarios, the lifetime of distribution equipment, LVR is negatively impacted through excessive operation. Furthermore, the proposed attack detection scheme is evaluated on four different attack severity scenarios, and the detection time is reported along with the attack onset time estimation.

6.5.1 Impact on Feeder's Daily Load Curve

On the other side at the main feeder, only the aggregated power demand data is available. This data is plotted in a daily feeder's load curve in Figure 6.9 considering normal operation and stealthy attack scenarios. For the power utility, the ideal case is to have the load curve as flat as possible, i.e., maintain the daily feeder loading at a constant rate. However, considering the stealthy attack scenario as shown in the figure, this curve is negatively impacted and becomes steeper.

6.5.2 Impact on a group of houses

This case study shows the impact of the attack on a group of residential houses in the case an adversary has compromised the IoT-enabled controller of the AC. In this attack

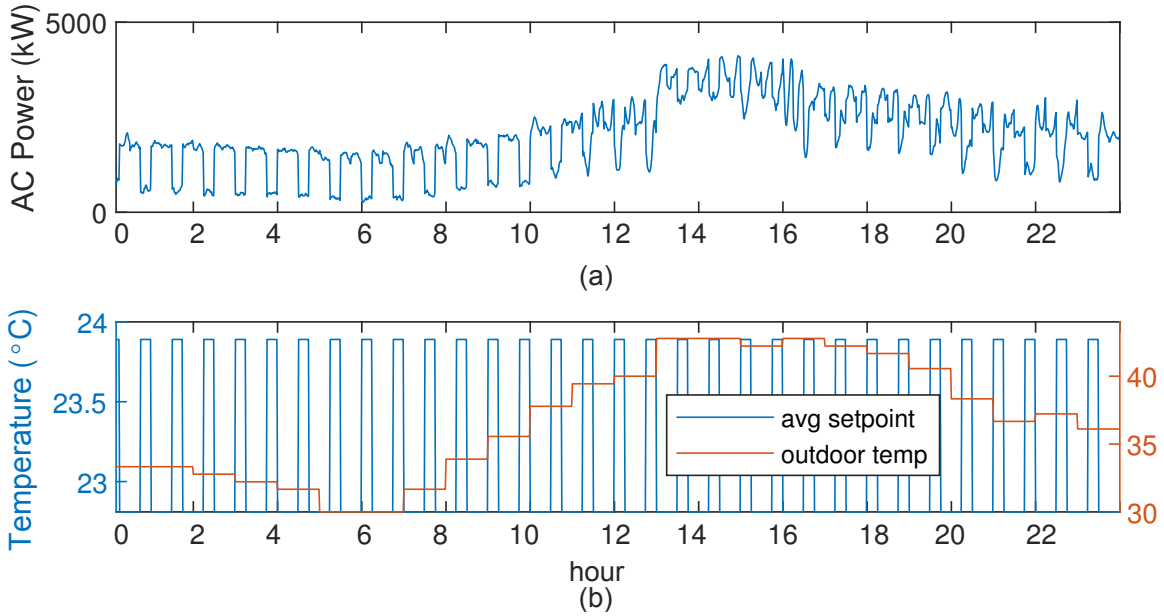


Figure 6.10: One day profile for a group of adjacent houses with compromised AC units: (a) The aggregated power demand, and (b) manipulated temperature setpoint vs. outdoor temperature.

scenario, the adversary manipulates the temperature setpoint values between 22°C and 24°C, as is shown in Figure 6.10-(b) for one day. The new setpoints are set in this range to maintain the comfort of the consumer, while the power demand fluctuated following the setpoints and the outdoor temperature as shown in Figure 6.10-(a).

6.5.3 Impact on bus voltage and LVR operation

Figure 6.11-(a) shows the daily voltage profile of bus-680 in the PDS during normal operations and three different attack scenarios in which the adversary has compromised 5%, 50%, and 75% of the IoT-enabled appliances. As shown in the figure, the voltage profile of bus-680 during low attack severity (5%) looks similar to the normal profile and remained within the acceptable range (i.e., between 0.95p.u. and 1.05p.u.). This can be attributed to the operation of LVR as can be noticed in Figure 6.11-(b) which shows that the relative daily LVR tap-changes-count ($\frac{\text{TCC}_{a=5\%}}{\text{TCC}_0}$) has increased to around 1.8 times the

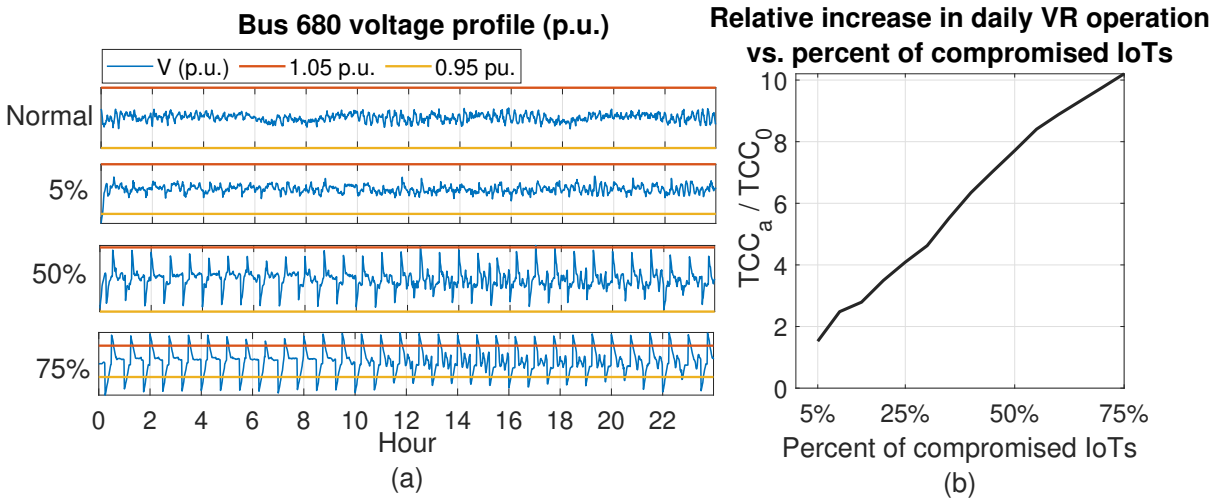


Figure 6.11: (a) Bus-680 voltage profile during normal and attack scenarios, and (b) Relative increase of LVR operation vs. percentage of compromised IoT-enabled appliances.

count during normal conditions (TCC_0).

Likewise, yet more harshly, when the number of compromised IoT-enabled appliances is increased to 50%, a significant voltage variation within the acceptable range is noticed with few violations. However, the relative daily operation of the LVR has significantly increased to nearly 8 times the TCC_0. Lastly, in an adverse scenario when 75% of the IoT-enabled appliances have been compromised, the network experienced voltage fluctuation and many voltage violations are noticed. In such an extreme case, although the LVR excessively operated to regulate the voltage, it could not cope with the severe violations. Such a scenario will most likely trigger the under/over protection devices in the PDS which will cause a power outage in some areas of the PDS's network.

6.5.4 Attack Detection

In this study, the proposed attack detection method is evaluated against the attacks controlling the compromised IoT-enabled appliances. Particularly, the detection of attacks is considered in scenarios when the attacker is able to control a set of devices that aggre-

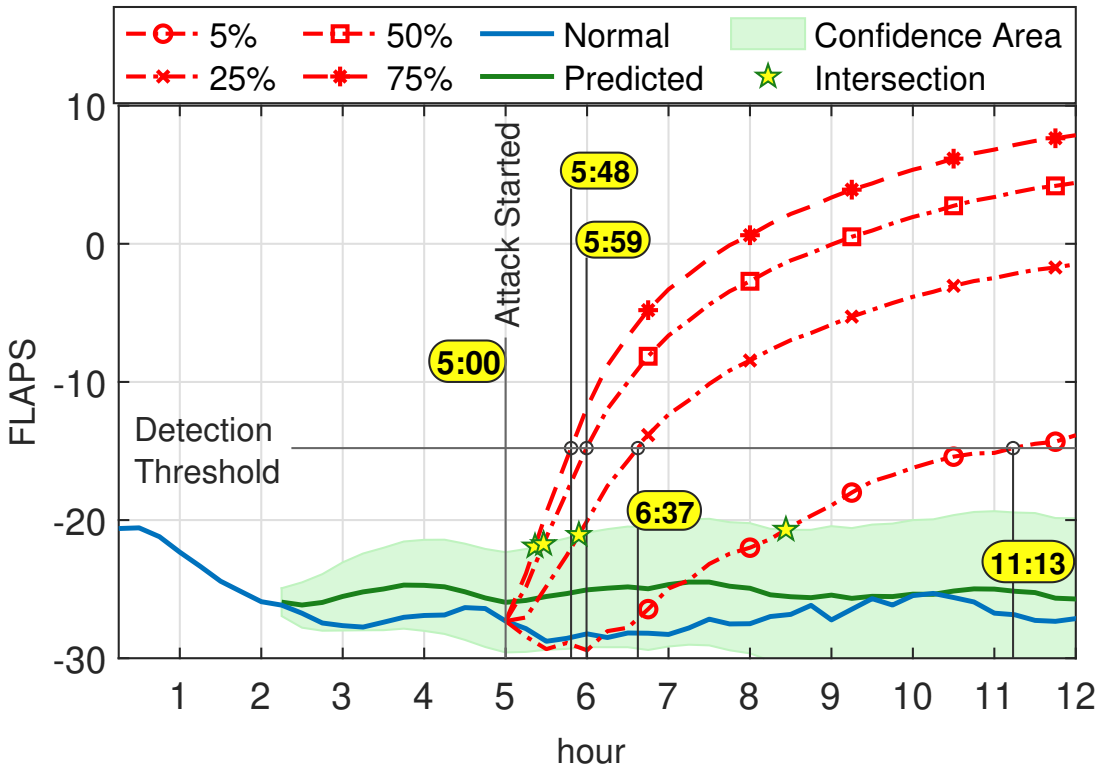


Figure 6.12: FLAPS index curve during normal and different attack severity conditions.

gates to (less severity) 5%, 25%, 50%, and 75% (most severity) of the total controllable demand. The detection performance is depicted in Figure 6.12 during 24 hours for the four attack scenarios in red curves along the normal scenario in blue.

All the attack scenarios started at 5:00 am, and as expected, the more the severity of the attack is the more rapidly the increase in the FLAPS curve will happen, and hence, the earlier the attack would be detected. In Figure 6.12, the attack detection time is identified from the point of intersection with the threshold line, i.e., 5:47 am, 5:58 am, 6:36 am, and 11:08 am for the 75%, 50%, 25%, and 5% of the attack scenarios, respectively. This can be explained considering that less severe attacks will have a smaller impact on the system compared to more severe attacks.

6.5.5 Attack Onset Time Estimation using Piecewise Regression

By observing the numerical results in Figure 6.12 during the various attack severity, it can be noticed that the FLAPS curve follows different characteristics once the attack is started. Hence, the curve can be divided into two segments: (i) Γ^{S_1} the segment of the FLAPS curve before the onset of the attack, as shown in blue (until 5:00 am), and (ii) Γ^{S_2} the segment of the FLAPS curve between the onset of the attack and the detection point, as shown in red. We propose that finding the correct split point, aka knot, of the curve will identify the onset time of the attack. Therefore, to find the split point, the following steps are followed once the attack detection approach is triggered:

• **Step 1**: Model each section of the FLAPS curve using two different functions. The proposed models include the polynomial for the first section, i.e., before the attack onset, and the linear model for the second section, i.e., between the onset of the attack and the detection point, as shown in Figure 6.13-(Top). These two models are described in equation (6.23) and equation (6.24), respectively.

$$\Psi_1(t) = a_0 + a_1 t + a_2 t^2 + ... + a_{n_1} t^{n_1} \tag{6.23}$$

$$\Psi_2(t) = b_0 + b_1 t \tag{6.24}$$

where n_1 represents the degree of the first polynomial model.

• **Step 2**: Find the split point that minimizes the total least-square fitting errors of the two models for the FLAPS values within the window of time $[t^{ad} - 24, t^{ad}]$, as shown in Figure 6.13-(Bottom). The time point t^{ad} is the attack detection time and $(t^{ad} - 24)$ is 24 hours before the attack is detected. During the least-square fitting, the polynomial degree n_1 is also identified.

The aforementioned steps are applied to the four attack severity levels and the results are presented in Table 6.3. As shown, the maximum estimation error is 5 minutes leading at 75% and lagging at 25% attack severity levels.

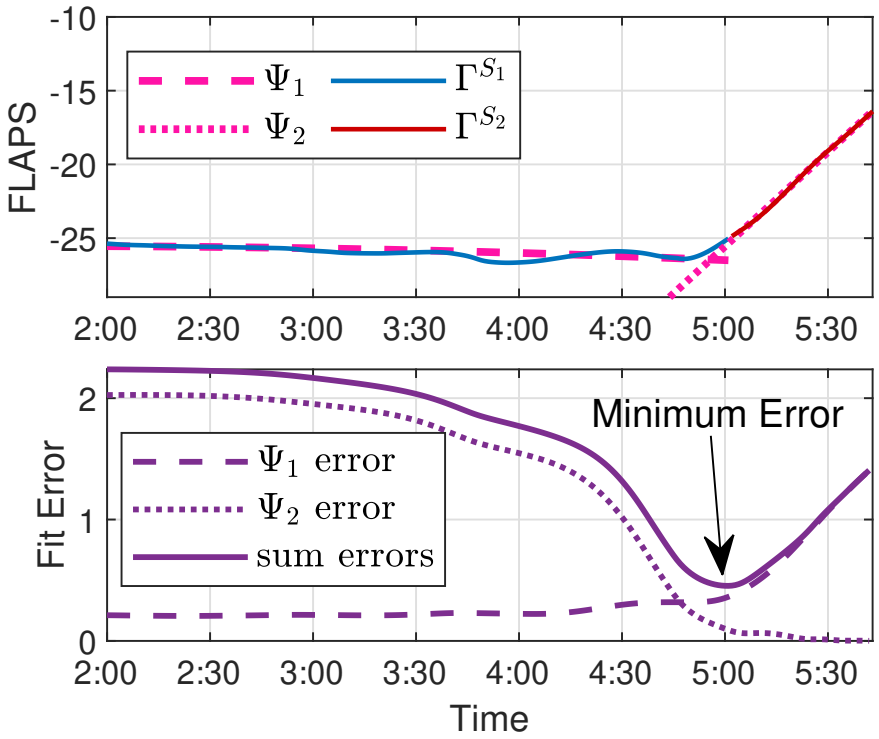


Figure 6.13: Attack onset time estimation. Top: the FLAPS curve segments Γ^{S_1} and Γ^{S_2} before and after the attack, respectively. Bottom: least-square fitting errors.

6.6 Conclusion

A new stealthy cyber–attack model is presented in this chapter for coordinated attacks on IoT-enabled smart home appliances targeting the reliability of PDSs. The model assumes that the operating conditions of the compromised appliances are constrained within the comfort levels to avoid triggering the attention of the consumers to unusual operations while participating in the attacks. The impact of the proposed attack model on the PDS

Table 6.3: The results of attack onset time estimation for attacks started at 5:00 am

Attack severity	5%	25%	50%	75%
Estimated onset time	5:04	5:05	5:03	4:55

is investigated and analyzed considering several attack severity scenarios. An effective real-time attack detection technique is proposed for the distribution system feeders using the power spectrum of the demand signal. The efficacy and feasibility of utilizing the proposed attack-detection scheme are demonstrated via practical simulations conducted on the IEEE 13-bus system. The proposed technique improves the resiliency of the PDS by detecting and alerting for stealthy attacks in a timely manner, thereby enabling the system to operate reliably and securely.

Chapter 7

Conclusion and Future Work

7.1 Summary and Conclusions

This thesis contributes to the global research on improving the security and resiliency of Smart Grids (SGs) and associated systems and components against cyber–physical attacks. Specifically, the contributions are divided into three domains based on the targeted system. The first one concerns securing the State Estimation (SE) module of the SG (Chapter 3). The research under the second domain, Chapters 4 and 5, aims to enhance the resiliency of the Integrated Power and Gas System (IPGS) facilities scheduler against cyber–attacks. Lastly, the third domain investigates the vulnerability of PDSs against load-altering attacks using a compromised set of IoT-enabled appliances (Chapter 6).

In Chapter 3, an efficient False Data Injection Attack (FDIA) approach is developed that imitates an intelligent adversary behavior searching for an optimal attack vector against SE modules which serves as the core of the Supervisory Control and Data Acquisition (SCADA) system. Simulation results on the IEEE 14-bus test system show that the proposed approach is able to find minimal attack vectors that an adversary can utilize to bypass the Bad Data Detection (BDD). The method also identifies successful attack vectors that work in real-time during a change between -100% to +100% in the standard system loading without the need to acquire additional measurements. Consequently, at-

tacks constructed using this approach require less computational time and resources by the adversary compared to the existing methods, which makes it suitable for generating attacks utilized for the analysis of cyber-security vulnerabilities and the design of resilient SE modules.

In Chapter 4, a framework model is developed to be utilized as a testbed for performing and analyzing the impact of cyber–attacks. The framework models steady-state power and gas flow operations, and presents a new financial interdependency operation scheduling model. The framework is validated on IEEE standard power distribution and transmission systems with variable generation and demand scenarios and high renewable penetration levels. The results indicate that Integrated Energy Systems (IESs) improves the balance between generation and demand in the system, especially during extreme renewables volatility.

In Chapter 5, anomaly-based attack detection and mitigation method is developed based on signal processing and machine-learning tools. The results show that the proposed method can detect attacks targeting external input data, whereas the accuracy is around 94.5% for detecting and correcting control commands communicated internally within the facility.

Chapter 6 investigates the vulnerability of PDSs to cyber–attacks that compromise a set of IoT-enabled loads, thereby impacting the efficiency and reliability of the PDSs. As such, a stealthy attack strategy is presented that minimizes the detection chances by preserving the compromised IoT-enabled appliances operating within the normal ranges. Accordingly, a novel real-time anomaly detection and prediction method is proposed based on demand power spectrum analysis and LSTM neural networks to counter stealthy attacks. A new index is proposed referred to as the FLAPS and utilized to estimate the attack onset time, which is then reported to the PDS's operator for further investigation and action. The impact of the proposed stealthy attack on the PDS is quantitatively analyzed considering the voltage violation cases and the wear and tear of the LVR.

7.2 Future Work

The potential cyber-security threats in SG have hindered the expansion and deployment of more cyber-based components and solutions. The cyber-security problem is very unpredictable and dynamic as new attack strategies are regularly found and as existing ones change. Efforts focusing on securing the Information and Communication Technologies (ICT) networks are not sufficient considering differences in the security objectives between ICT networks and SGs. Additionally, the types of cyber–attacks that have already occurred suggest that energy sector vulnerabilities may exist. As a result, it is a big technical challenge to research cyber-security concerns in applications involving SGs [171].

Considering the research work presented in this thesis under the three domains, the following future research ideas can be investigated to further enhance the proposed methods:

- Securing the SE is critical to SG's operation and expansion plans. Thus, a potential point of research will be to develop intelligent anomaly detection-based approaches to improve the resiliency of SE modules in SGs. The approach shall consider the long-term correlation between loads across the system buses and the continuous changes in power systems structure (i.e., due to topology and resource variability). Data pre-processing techniques, such as feature selection, will be explored to improve the attack detection performance. The countermeasure developed in this objective enhances the deployment of machine learning-based detection methods.

- In the proposed detection methods for the attacks on the primary and secondary data of IPGS, attacks that do not violate system limits may go undetected. However, considering a stealthy approach, their long-run impact on the IPGS facility progressively increases causing, e.g., losses in revenue. A potential future research idea will be to generate such attack scenarios and propose a custom detection approach based on the modeling system's parameter variation patterns. Using these patterns, one will be able to identify anomalous changes.

- Propose resilient mitigation approaches to countermeasure the attacks against PDSs through compromised IoT-based Distributed Energy Resources (DERs). For instance, investigating approaches to provide a fast response when sudden load changes are experienced due to cyber–attacks, such as the deployment of super-capacitor banks.

Besides the aforementioned concrete ideas, the future research work in SG can be grouped under five categories:

1. Investigating methods to exploit SG vulnerabilities which becomes more difficult with the integration of multiple systems and deployment of independent energy resources, such as renewables, that increase the level of uncertainty in the SG.

2. Evaluate the impact of cyber–attacks on SG operation considering the distributed architecture where the complete real-time information about the SG status is not available to a single entity.

3. Propose novel attack detection algorithms using machine learning and statistical approaches.

4. Develop defense mechanisms that follow both mitigation and remedy actions to alleviate the impact of attacks.

5. Improve the standardization and regulation of IoT deployment in SG infrastructure. Although many IoT devices can communicate with one another, there are no IoT universal standards. Existing IoT device manufacturers must choose between various frameworks, and usually, priority is given to connectivity over security. While consumers must determine whether the devices they desire are compatible with the ones they already own. This leaves the majority of IoT devices with loose security procedures and encryption techniques, making them easy to be hacked. Therefore, it is difficult to design IoT-based SG applications and devices without considering following unified standards with cyber-security in focus.

Bibliography

[1] X. Fang et al. “Smart Grid–The New and Improved Power Grid: A Survey”. In: *IEEE Communications Surveys Tutorials* 14.4 (2011), pp. 944–980 (cit. on p. 1).

[2] P. D. Lund et al. “Review of energy system flexibility measures to enable high levels of variable renewable electricity”. In: *Renewable and sustainable energy reviews* 45 (2015), pp. 785–807 (cit. on p. 1).

[3] E. Guelpa et al. “Towards future infrastructures for sustainable multi-energy systems: A review”. In: *Energy* 184 (2019), pp. 2–21 (cit. on pp. 2, 78).

[4] S. Al-Sarawi et al. “Internet of Things Market Analysis Forecasts, 2020–2030”. In: *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*. 2020, pp. 449–453 (cit. on p. 2).

[5] Q. Shafi. “Cyber Physical Systems Security: A Brief Survey”. In: *2012 12th International Conference on Computational Science and Its Applications*. 2012, pp. 146–150 (cit. on p. 2).

[6] R. Langner. “Stuxnet: Dissecting a Cyberwarfare Weapon”. In: *IEEE Security Privacy* 9.3 (May 2011), pp. 49–51 (cit. on p. 2).

[7] N. Falliere. *Stuxnet Introduces the First Known Rootkit for Industrial Control Systems*. Aug. 2010. URL: https://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices (visited on 08/2019) (cit. on p. 2).

[8] E. Nakashima. *Russian hackers suspected in attack that blacked out parts of Ukraine*. Jan. 5, 2016. URL: https://www.washingtonpost.com/world/national-security/russian-hackers-suspected-in-attack-that-blacked-out-parts-of-ukraine/2016/01/05/4056a4dc-b3de-11e5-a842-0feb51d1d124_story.html (visited on 08/2019) (cit. on p. 2).

[9] Y. Xue and X. Yu. "Beyond Smart Grid—A Cyber–Physical–Social System in Energy Future". In: *Proc. IEEE* 105.12 (Dec. 2017), pp. 2290–2292 (cit. on pp. 2, 6, 78).

[10] H. He and J. Yan. "Cyber-physical attacks and defences in the smart grid: a survey". In: *IET Cyber-Physical Systems: Theory & Applications* 1.1 (2016), pp. 13–27 (cit. on pp. 3, 23, 25, 29).

[11] K. Stouffer et al. "Guide to Industrial Control Systems (ICS) Security". In: *NIST Special Publication* 800 (2015), p. 82 (cit. on p. 3).

[12] S. Sridhar and M. Govindarasu. "Model-Based Attack Detection and Mitigation for Automatic Generation Control". In: *IEEE Transactions on Smart Grid* 5.2 (2014), pp. 580–591 (cit. on p. 5).

[13] A. Anwar, A. N. Mahmood, and Z. Tari. "Identification of vulnerable node clusters against false data injection attack in an AMI based smart grid". In: *Information Systems* 53 (2015), pp. 201–212 (cit. on p. 5).

[14] H. Ye et al. "Transmission Line Rating Attack in Two-Settlement Electricity Markets". In: *IEEE Transactions on Smart Grid* 7.3 (2016), pp. 1346–1355 (cit. on p. 5).

[15] A. Sargolzaei, K. Yen, and M. Abdelghani. "Delayed inputs attack on load frequency control in smart grid". In: *ISGT 2014*. 2014, pp. 1–5 (cit. on p. 5).

[16] E. Hammad et al. "A Class of Switching Exploits Based on Inter-Area Oscillations". In: *IEEE Transactions on Smart Grid* 9.5 (2018), pp. 4659–4668 (cit. on p. 5).

[17] Y. Liu, P. Ning, and M. K. Reiter. "False data injection attacks against state estimation in electric power grids". In: *ACM Transactions on Information and System Security (TISSEC)* 14.1 (2011), p. 13 (cit. on pp. 5, 26, 36).

[18] X. Liu et al. "Masking Transmission Line Outages via False Data Injection Attacks". In: *IEEE Transactions on Information Forensics and Security* 11.7 (2016), pp. 1592–1602 (cit. on p. 5).

[19] X. Liu and Z. Li. "False data attacks against AC state estimation with incomplete network information". In: *IEEE Transactions on smart grid* 8.5 (2016), pp. 2239–2248 (cit. on pp. 5, 26).

[20] P. Zhuang, R. Deng, and H. Liang. “False Data Injection Attacks Against State Estimation in Multiphase and Unbalanced Smart Distribution Systems”. In: *IEEE Transactions on Smart Grid* 10.6 (2019), pp. 6000–6013 (cit. on pp. 5, 30).

[21] W. Yao et al. “Impact of GPS Signal Loss and Its Mitigation in Power System Synchronized Measurement Devices”. In: *IEEE Transactions on Smart Grid* 9.2 (2018), pp. 1141–1149 (cit. on p. 5).

[22] W. Yao et al. “A Novel Method for Phasor Measurement Unit Sampling Time Error Compensation”. In: *IEEE Transactions on Smart Grid* 9.2 (2018), pp. 1063–1072 (cit. on p. 5).

[23] G. Hug and J. A. Giampapa. “Vulnerability Assessment of AC state Estimation with Respect to False Data Injection Cyber-Attacks”. In: *IEEE Transactions on smart grid* 3.3 (2012), pp. 1362–1370 (cit. on pp. 5, 26, 37).

[24] M. A. Rahman and H. Mohsenian-Rad. “False data injection attacks against nonlinear state estimation in smart power grids”. In: *2013 IEEE Power & Energy Society General Meeting*. IEEE. 2013, pp. 1–5 (cit. on pp. 5, 26, 36).

[25] R. Deng et al. “False Data Injection on State Estimation in Power Systems—Attacks, Impacts, and Defense: A Survey”. In: *IEEE Transactions on Industrial Informatics* 13.2 (2017), pp. 411–423 (cit. on pp. 5, 27).

[26] S. Mei et al. “Paving the way to smart micro energy grid: concepts, design principles, and engineering practices”. In: *CSEE Journal of Power and Energy Systems* 3.4 (Dec. 2017), pp. 440–449 (cit. on pp. 6, 15).

[27] W. Shengyu et al. “Review on interdependency modeling of integrated energy system”. In: *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*. Nov. 2017, pp. 1–6 (cit. on pp. 6, 15).

[28] M. Shahidehpour, Yong Fu, and T. Wiedman. “Impact of Natural Gas Infrastructure on Electric Power Systems”. In: *Proceedings of the IEEE* 93.5 (May 2005), pp. 1042–1056 (cit. on pp. 6, 15).

[29] M. Urbina and Z. Li. “A Combined Model for Analyzing the Interdependency of Electrical and Gas Systems”. In: *2007 39th North American Power Symposium*. Sept. 2007, pp. 468–472 (cit. on pp. 6, 15).

[30] C. M. Correa-Posada and P. Sánchez-Martın. “Security-Constrained Optimal Power and Natural-Gas Flow”. In: *IEEE Transactions on Power Systems* 29.4 (July 2014), pp. 1780–1787 (cit. on pp. 6, 15, 88).

[31] T. Li, M. Eremia, and M. Shahidehpour. “Interdependency of Natural Gas Network and Power System Security”. In: *IEEE Transactions on Power Systems* 23.4 (Nov. 2008), pp. 1817–1824 (cit. on pp. 6, 15).

[32] M. P. Barrett et al. “Framework for improving critical infrastructure cybersecurity version 1.1”. In: (2018) (cit. on p. 7).

[33] C. Barreto, H. Neema, and X. Koutsoukos. “Attacking Electricity Markets Through IoT Devices”. In: *Computer* 53.5 (2020), pp. 55–62 (cit. on p. 7).

[34] C. Barreto and A. A. Cárdenas. “Impact of the Market Infrastructure on the Security of Smart Grids”. In: *IEEE Transactions on Industrial Informatics* 15.7 (2019), pp. 4342–4351 (cit. on pp. 7, 29).

[35] S. Soltan, P. Mittal, and H. V. Poor. “BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid”. In: *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 15–32. ISBN: 978-1-939133-04-5 (cit. on p. 7).

[36] B. Huang, A. A. Cardenas, and R. Baldick. “Not Everything is Dark and Gloomy: Power Grid Protections against IoT Demand Attacks”. In: *Proceedings of the 28th USENIX Conference on Security Symposium*. SEC’19. Santa Clara, CA, USA: USENIX Association, 2019, pp. 1115–1132. ISBN: 9781939133069 (cit. on p. 7).

[37] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad. “Dynamic Load Altering Attacks Against Power System Stability: Attack Models and Protection Schemes”. In: *IEEE Transactions on Smart Grid* 9.4 (2018), pp. 2862–2872 (cit. on p. 8).

[38] S. Acharya, Y. Dvorkin, and R. Karri. “Public Plug-in Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable?” In: *IEEE Transactions on Smart Grid* 11.6 (2020), pp. 5099–5113 (cit. on p. 8).

[39] S. Lakshminarayana, S. Adhikari, and C. Maple. “Analysis of IoT-Based Load Altering Attacks Against Power Grids Using the Theory of Second-Order Dynamical Systems”. In: *IEEE Transactions on Smart Grid* 12.5 (2021), pp. 4415–4425 (cit. on p. 8).

[40] P. Srikantha, J. Liu, and J. Samarabandu. “A Novel Distributed and Stealthy Attack on Active Distribution Networks and a Mitigation Strategy”. In: *IEEE Transactions on Industrial Informatics* 16.2 (2020), pp. 823–831 (cit. on p. 8).

[41] J. Ospina et al. “On the Feasibility of Load-Changing Attacks in Power Systems During the COVID-19 Pandemic”. In: *IEEE Access* 9 (2021), pp. 2545–2563 (cit. on p. 8).

[42] A. Muir and J. Lopatto. “Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations”. In: (2004) (cit. on p. 12).

[43] A. A. Chowdhury, S. K. Agarwal, and D. O. Koval. “Reliability modeling of distributed generation in conventional distribution systems planning and analysis”. In: *Conference Record of the 2002 IEEE Industry Applications Conference. 37th IAS Annual Meeting (Cat. No.02CH37344)*. Vol. 2. Oct. 2002, 1089–1094 vol.2 (cit. on p. 12).

[44] H. Farhangi. “The path of the smart grid”. In: *IEEE Power and Energy Magazine* 8.1 (Jan. 2010), pp. 18–28 (cit. on p. 13).

[45] J. P. Lopes et al. “Integrating distributed generation into electric power systems: A review of drivers, challenges and opportunities”. In: *Electric Power Systems Research* 77.9 (2007). Distributed Generation, pp. 1189–1203. ISSN: 0378-7796 (cit. on p. 13).

[46] M. H. Nehrir et al. “A Review of Hybrid Renewable/Alternative Energy Systems for Electric Power Generation: Configurations, Control, and Applications”. In: *IEEE Transactions on Sustainable Energy* 2.4 (Oct. 2011), pp. 392–403 (cit. on p. 13).

[47] V. Zare. “A comparative thermodynamic analysis of two tri-generation systems utilizing low-grade geothermal energy”. In: *Energy Conversion and Management* 118 (2016), pp. 264–274 (cit. on p. 13).

[48] K. Rajashekara. “Hybrid fuel-cell strategies for clean power generation”. In: *IEEE Transactions on industry Applications* 41.3 (2005), pp. 682–689 (cit. on p. 13).

[49] H. Gharavi and R. Ghafurian. “Smart Grid: The Electric Energy System of the Future [Scanning the Issue]”. In: *Proceedings of the IEEE* 99.6 (June 2011), pp. 917–921 (cit. on p. 13).

[50] R. Bayindir et al. “Smart grid technologies and applications”. In: *Renewable and Sustainable Energy Reviews* 66 (2016), pp. 499–516. ISSN: 1364-0321 (cit. on p. 13).

[51] CIGRE. *Impact of Increasing Contribution of Dispersed Generation on the Power System*. Report. Working Group Report 137, Feb. 1999 (cit. on p. 13).

[52] E. J. Coster et al. “Integration issues of distributed generation in distribution grids”. In: *Proceedings of the IEEE* 99.1 (2010), pp. 28–39 (cit. on p. 14).

[53] M. Ghiasi. “Detailed study, multi-objective optimization, and design of an AC-DC smart microgrid with hybrid renewable energy resources”. In: *Energy* 169 (2019), pp. 496–507 (cit. on p. 14).

[54] M. D. Al-Falahi, S. D. Jayasinghe, and H. Enshaei. “Hybrid algorithm for optimal operation of hybrid energy systems in electric ferries”. In: *Energy* 187 (2019), p. 115923 (cit. on p. 14).

[55] S. M. Dawoud, X. Lin, and M. I. Okba. “Hybrid renewable microgrid optimization techniques: A review”. In: *Renewable and Sustainable Energy Reviews* 82 (2018), pp. 2039–2052 (cit. on p. 14).

[56] A. Zakariazadeh, S. Jadid, and P. Siano. “Integrated operation of electric vehicles and renewable generation in a smart distribution system”. In: *Energy Conversion and Management* 89 (2015), pp. 99–110 (cit. on p. 14).

[57] F. A. Khan, N. Pal, and S. Saeed. “Review of solar photovoltaic and wind hybrid energy systems for sizing strategies optimization techniques and cost analysis methodologies”. In: *Renewable and Sustainable Energy Reviews* 92 (2018), pp. 937–947 (cit. on p. 14).

[58] R. Hosseinalizadeh et al. “Economic sizing of a hybrid (PV–WT–FC) renewable energy system (HRES) for stand-alone usages by an optimization-simulation model: Case study of Iran”. In: *Renewable and Sustainable Energy Reviews* 54 (2016), pp. 139–150 (cit. on p. 14).

[59] N. Li and K. W. Hedman. “Economic Assessment of Energy Storage in Systems With High Levels of Renewable Resources”. In: *IEEE Transactions on Sustainable Energy* 6.3 (July 2015), pp. 1103–1111 (cit. on p. 14).

[60] L. Valverde, F. Rosa, and C. Bordons. “Design, Planning and Management of a Hydrogen-Based Microgrid”. In: *IEEE Transactions on Industrial Informatics* 9.3 (Aug. 2013), pp. 1398–1404 (cit. on p. 14).

[61] M. S. Whittingham. “History, Evolution, and Future Status of Energy Storage”. In: *Proceedings of the IEEE* 100.Special Centennial Issue (May 2012), pp. 1518–1534 (cit. on p. 14).

[62] A. Kulkarni, J. Payne, and P. Mistretta. “Integrating SCADA, Load Shedding, and High-Speed Controls on an Ethernet Network at a North American Refinery”. In: *IEEE Transactions on Industry Applications* 51.2 (Mar. 2015), pp. 1360–1368 (cit. on p. 15).

[63] Q. Zeng et al. “Steady-state analysis of the integrated natural gas and electric power system with bi-directional energy conversion”. In: *Applied Energy* 184 (2016), pp. 1483–1492 (cit. on p. 15).

[64] S. Clegg and P. Mancarella. “Storing renewables in the gas network: modelling of power-to-gas seasonal storage flexibility in low-carbon power systems”. In: *IET Generation, Transmission & Distribution* 10.3 (2016), pp. 566–575 (cit. on p. 16).

[65] D. Alkano and J. M. A. Scherpen. “Distributed Supply Coordination for Power-to-Gas Facilities Embedded in Energy Grids”. In: *IEEE Transactions on Smart Grid* 9.2 (Mar. 2018), pp. 1012–1022 (cit. on p. 16).

[66] J. H. Huang et al. “Assessment of an integrated energy system embedded with power-to-gas plant”. In: *2016 IEEE Innovative Smart Grid Technologies - Asia (ISGT-Asia)*. Nov. 2016, pp. 196–201 (cit. on p. 16).

[67] C. He et al. “Robust Co-Optimization Scheduling of Electricity and Natural Gas Systems via ADMM”. In: *IEEE Transactions on Sustainable Energy* 8.2 (Apr. 2017), pp. 658–670 (cit. on p. 16).

[68] H. Khani and H. E. Z. Farag. “Optimal Day–Ahead Scheduling of Power–to–Gas Energy Storage and Gas Load Management in Wholesale Electricity and Gas Markets”. In: *IEEE Transactions on Sustainable Energy* 9.2 (Apr. 2018), pp. 940–951 (cit. on pp. 16, 18, 88).

[69] Y. Li et al. “Optimal Operation Strategy for Integrated Power-to-Gas and Natural Gas Generating Unit Facilities”. In: *IEEE Transactions on Sustainable Energy* (2018), pp. 1–1 (cit. on p. 16).

[70] S. Clegg and P. Mancarella. “Integrated Modeling and Assessment of the Operational Impact of Power-to-Gas (P2G) on Electrical and Gas Transmission Networks”. In: *IEEE Trans. on Sustainable Energy* 6.4 (Oct. 2015), pp. 1234–1244. ISSN: 1949-3029 (cit. on p. 17).

[71] H. Khani, N. El-Taweel, and H. E. Z. Farag. “Power Congestion Management in Integrated Electricity and Gas Distribution Grids”. In: *IEEE Systems Journal* (2018), pp. 1–12 (cit. on pp. 17, 64, 65).

[72] H. Khani, N. El-Taweel, and H. E. Farag. “Real-time optimal management of reverse power flow in integrated power and gas distribution grids under large renewable power penetration”. In: *IET Generation, Transmission & Distribution* 12 (10 May 2018), 2325–2331(6) (cit. on p. 17).

[73] H. Khani, N. A. El-Taweel, and H. E. Z. Farag. “Power Loss Alleviation in Integrated Power and Natural Gas Distribution Grids”. In: *IEEE Transactions on Industrial Informatics* 15.12 (2019), pp. 6220–6230 (cit. on p. 17).

[74] N. A. El-Taweel, H. Khani, and H. E. Farag. “Voltage regulation in active power distribution systems integrated with natural gas grids using distributed electric and gas energy resources”. In: *International Journal of Electrical Power & Energy Systems* 106 (2019), pp. 561–571 (cit. on p. 17).

[75] M. Lehner et al. *Power-to-gas: technology and business models*. Springer, 2014 (cit. on p. 18).

[76] A. Buttler and H. Spliethoff. “Current status of water electrolysis for energy storage, grid balancing and sector coupling via power-to-gas and power-to-liquids: A review”. In: *Renewable and Sustainable Energy Reviews* 82 (2018), pp. 2440–2454 (cit. on p. 18).

[77] F. Bhuiyan and A. Yazdani. “Reliability assessment of a wind-power system with integrated energy storage”. In: *IET Renewable Power Generation* 4.3 (2010), pp. 211–220 (cit. on p. 20).

[78] A. Belderbos. “Storage via power-to-gas in future energy systems: The need for synthetic fuel storage in systems with high shares of intermittent renewables”. KU Leuven University, Leuven, Belgium, 2019 (cit. on p. 20).

[79] Hydrogenics Corporation. “North America’s First Multi–Megawatt Power–to–Gas Facility Begins Operations”. In: *Hydrogenics Corporation News* (Jan. 11, 2019) (cit. on p. 20).

[80] NS Energy Staff Writer. “Air Liquide inaugurates 20MW PEM electrolyser in Québec, Canada”. In: *NS Energy News* (Jan. 27, 2021) (cit. on p. 20).

[81] I. D. de Cerio Mendaza et al. “Optimal sizing and placement of power–to–gas systems in future active distribution networks”. In: *2015 IEEE Innovative Smart Grid Technologies - Asia (ISGT ASIA)*. Nov. 2015, pp. 1–6 (cit. on pp. 20, 58).

[82] M. Bailera et al. “Power to Gas projects review: Lab, pilot and demo plants for storing renewable energy and CO2”. In: *Renewable and Sustainable Energy Reviews* 69 (2017), pp. 292–312 (cit. on p. 20).

[83] M. Faheem et al. “Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges”. In: *Comput. Sci. Rev.* 30 (2018), pp. 1–30 (cit. on p. 21).

[84] R. Deng, P. Zhuang, and H. Liang. “CCPA: Coordinated Cyber-Physical Attacks and Countermeasures in Smart Grid”. In: *IEEE Transactions on Smart Grid* 8.5 (2017), pp. 2420–2430 (cit. on p. 21).

[85] G. Loukas. “4 - Cyber-Physical Attacks on Industrial Control Systems”. In: *Cyber-Physical Attacks*. Ed. by G. Loukas. Boston: Butterworth-Heinemann, 2015, pp. 105–144. ISBN: 978-0-12-801290-1 (cit. on p. 22).

[86] S. Behal and K. Kumar. “Characterization and Comparison of DDoS Attack Tools and Traffic Generators: A Review”. In: *Int. J. Netw. Secur.* 19 (2017), pp. 383–393 (cit. on p. 22).

[87] G. Liang et al. “A Review of False Data Injection Attacks Against Modern Power Systems”. In: *IEEE Transactions on Smart Grid* 8.4 (2017), pp. 1630–1638 (cit. on pp. 23, 27, 78).

[88] X. Liu et al. “Cyber Attacks Against the Economic Operation of Power Systems: A Fast Solution”. In: *IEEE Transactions on Smart Grid* 8.2 (Mar. 2017), pp. 1023–1025 (cit. on p. 23).

[89] X. Liu et al. “Power System Risk Assessment in Cyber Attacks Considering the Role of Protection Systems”. In: *IEEE Transactions on Smart Grid* 8.2 (Mar. 2017), pp. 572–580 (cit. on p. 24).

[90] C. Moya and J. Wang. “Developing correlation indices to identify coordinated cyber-attacks on power grids”. In: *IET Cyber-Physical Systems: Theory Applications* 3.4 (Dec. 2018), pp. 178–186 (cit. on p. 24).

[91] G. Huang et al. “Cyber-Constrained Optimal Power Flow Model for Smart Grid Resilience Enhancement”. In: *IEEE Transactions on Smart Grid* 10.5 (Sept. 2018), pp. 5547–5555 (cit. on p. 24).

[92] Y. Cui et al. “A Measurement Source Authentication Methodology for Power System Cyber Security Enhancement”. In: *IEEE Transactions on Smart Grid* 9.4 (July 2018), pp. 3914–3916 (cit. on p. 24).

[93] H. Lin, Z. Kalbarczyk, and R. K. Iyer. "RAINCOAT: RAndomization of Network Communication in Power Grid Cyber INfrastructure to Mislead Attackers". In: *IEEE Transactions on Smart Grid* 10.5 (Sept. 2019), pp. 4893–4906 (cit. on p. 24).

[94] M. Zeraati, Z. Aref, and M. A. Latify. "Vulnerability Analysis of Power Systems Under Physical Deliberate Attacks Considering Geographic-Cyber Interdependence of the Power System and Communication Network". In: *IEEE Systems Journal* 12.4 (Dec. 2018), pp. 3181–3190 (cit. on p. 24).

[95] A. Di Giorgio et al. "Robust protection scheme against cyber–physical attacks in power systems". In: *IET Control Theory Applications* 12.13 (2018), pp. 1792–1801 (cit. on p. 24).

[96] G. Liang et al. "Distributed Blockchain–Based Data Protection Framework for Modern Power Systems Against Cyber Attacks". In: *IEEE Transactions on Smart Grid* 10.3 (May 2019), pp. 3162–3173 (cit. on p. 24).

[97] Y. He, G. J. Mendis, and J. Wei. "Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism". In: *IEEE Transactions on Smart Grid* 8.5 (Sept. 2017), pp. 2505–2516 (cit. on pp. 25, 86).

[98] H. Karimipour et al. "A Deep and Scalable Unsupervised Machine Learning System for Cyber-Attack Detection in Large-Scale Smart Grids". In: *IEEE Access* 7 (May 2019), pp. 80778–80788 (cit. on pp. 25, 86).

[99] W. Li, L. Xie, and Z. Wang. "Two-Loop Covert Attacks Against Constant Value Control of Industrial Control Systems". In: *IEEE Transactions on Industrial Informatics* 15.2 (Feb. 2019), pp. 663–676 (cit. on pp. 25, 78, 86).

[100] J. J. Q. Yu, Y. Hou, and V. O. K. Li. "Online False Data Injection Attack Detection With Wavelet Transform and Deep Neural Networks". In: *IEEE Transactions on Industrial Informatics* 14.7 (July 2018), pp. 3271–3280 (cit. on pp. 25, 86).

[101] M. Esmalifalak et al. "Detecting Stealthy False Data Injection Using Machine Learning in Smart Grid". In: *IEEE Systems Journal* 11.3 (Sept. 2017), pp. 1644–1652 (cit. on pp. 25, 27, 86).

[102] T. T. Kim and H. V. Poor. "Strategic protection against data injection attacks on power grids". In: *IEEE Transactions on Smart Grid* 2.2 (2011), pp. 326–333 (cit. on p. 26).

[103] O. Kosut et al. "Malicious data attacks on the smart grid". In: *IEEE Transactions on Smart Grid* 2.4 (2011), pp. 645–658 (cit. on p. 26).

[104] Q. Yang et al. “On a hierarchical false data injection attack on power system state estimation”. In: *2011 IEEE Global Telecommunications Conference-GLOBECOM 2011*. IEEE. 2011, pp. 1–5 (cit. on p. 27).

[105] O. Vukovic et al. “Network-aware mitigation of data integrity attacks on power system state estimation”. In: *IEEE Journal on Selected Areas in Communications* 30.6 (2012), pp. 1108–1118 (cit. on p. 27).

[106] Y. Wang et al. “A novel data analytical approach for false data injection cyber–physical attack mitigation in smart grids”. In: *IEEE Access* 5 (2017), pp. 26022–26033 (cit. on p. 27).

[107] S. Yin et al. “State estimation in nonlinear system using sequential evolutionary filter”. In: *IEEE Transactions on Industrial Electronics* 63.6 (2016), pp. 3786–3794 (cit. on p. 27).

[108] Y.-F. Huang et al. “State estimation in electric power grids: Meeting new challenges presented by the requirements of the future grid”. In: *IEEE Signal Processing Magazine* 29.5 (2012), pp. 33–43 (cit. on p. 27).

[109] S. Sinha. *State of IoT 2021: Number of connected IoT devices growing 9% to 12.3 billion globally, cellular IoT now surpassing 2 billion*. Sept. 22, 2021 (cit. on p. 27).

[110] A. Humayed et al. “Cyber-Physical Systems Security—A Survey”. In: *IEEE Internet of Things Journal* 4.6 (2017), pp. 1802–1831 (cit. on p. 27).

[111] A. Al-Fuqaha et al. “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications”. In: *IEEE Communications Surveys Tutorials* 17.4 (2015), pp. 2347–2376 (cit. on p. 27).

[112] H. ElSawy, M. A. Kishk, and M.-S. Alouini. “Spatial Firewalls: Quarantining Malware Epidemics in Large-Scale Massive Wireless Networks”. In: *IEEE Communications Magazine* 58.9 (2020), pp. 32–38 (cit. on p. 28).

[113] E. Fernandes, J. Jung, and A. Prakash. “Security Analysis of Emerging Smart Home Applications”. In: *2016 IEEE Symposium on Security and Privacy (SP)*. 2016, pp. 636–654 (cit. on p. 28).

[114] I. Agadakos et al. “Jumping the Air Gap: Modeling Cyber-Physical Attack Paths in the Internet-of-Things”. In: *Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy*. CPS ’17. Dallas, Texas, USA: Association for Computing Machinery, 2017, pp. 37–48. ISBN: 9781450353946 (cit. on p. 28).

[115] J. Porter. *Security researchers expose new Alexa and Google Home vulnerability.* Oct. 21, 2019 (cit. on p. 28).

[116] S. Khandelwal. *Bluetooth Hack Affects 20 Million Amazon Echo and Google Home Devices.* Nov. 16, 2017 (cit. on p. 28).

[117] T. Riley. *The Cybersecurity 202: Smart home devices with known security flaws are still on the market, researchers say.* Feb. 4, 2021 (cit. on p. 28).

[118] A. Dabrowski, J. Ullrich, and E. R. Weippl. "Grid Shock: Coordinated Load-Changing Attacks on Power Grids: The Non-Smart Power Grid is Vulnerable to Cyber Attacks as Well". In: *Proceedings of the 33rd Annual Computer Security Applications Conference.* ACSAC 2017. Orlando, FL, USA: Association for Computing Machinery, 2017, pp. 303–314. ISBN: 9781450353458 (cit. on p. 28).

[119] M. Antonakakis et al. "Understanding the Mirai Botnet". In: *26th USENIX security symposium (USENIX Security 17).* 2017, pp. 1093–1110 (cit. on p. 29).

[120] G. Gallopeni et al. "A Practical Analysis on Mirai Botnet Traffic". In: *2020 IFIP Networking Conference (Networking).* 2020, pp. 667–668 (cit. on p. 29).

[121] Y. Kabalci et al. "Internet of things applications as energy internet in smart grids and smart environments". In: *Electronics* 8.9 (2019), p. 972 (cit. on p. 29).

[122] S. Tan et al. "New Challenges in the Design of Microgrid Systems: Communication Networks, Cyberattacks, and Resilience". In: *IEEE Electrification Magazine* 8.4 (2020), pp. 98–106 (cit. on p. 29).

[123] J. Leitão et al. "A Survey on Home Energy Management". In: *IEEE Access* 8 (2020), pp. 5699–5722 (cit. on p. 29).

[124] J. L. Gallardo, M. A. Ahmed, and N. Jara. "LoRa IoT-Based Architecture for Advanced Metering Infrastructure in Residential Smart Grid". In: *IEEE Access* 9 (2021), pp. 124295–124312 (cit. on p. 29).

[125] B. Hartono, S. P. Mursid, and S. Prajogo. "Review: Home energy management system in a Smart Grid scheme to improve reliability of power systems". In: *IOP Conference Series: Earth and Environmental Science* 105 (Jan. 2018), p. 012081 (cit. on p. 29).

[126] N. Komninos, E. Philippou, and A. Pitsillides. "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures". In: *IEEE Communications Surveys Tutorials* 16.4 (2014), pp. 1933–1954 (cit. on p. 29).

[127] H. Lin and N. W. Bergmann. "IoT Privacy and Security Challenges for Smart Home Environments". In: *Information* 7.3 (2016). ISSN: 2078-2489 (cit. on p. 29).

[128] Q. Jing et al. "Security of the Internet of Things: perspectives and challenges". In: *Wireless Networks* 20.8 (2014), pp. 2481–2501 (cit. on p. 29).

[129] R. Heartfield et al. "A taxonomy of cyber–physical threats and impact in the smart home". In: *Computers and Security* 78 (2018), pp. 398–428. ISSN: 0167-4048 (cit. on p. 29).

[130] J. Wurm et al. "Security analysis on consumer and industrial IoT devices". In: *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*. 2016, pp. 519–524 (cit. on p. 30).

[131] Y. Liu, S. Hu, and A. Y. Zomaya. "The Hierarchical Smart Home Cyberattack Detection Considering Power Overloading and Frequency Disturbance". In: *IEEE Transactions on Industrial Informatics* 12.5 (2016), pp. 1973–1983 (cit. on p. 30).

[132] C.-C. Sun et al. "Intrusion Detection for Cybersecurity of Smart Meters". In: *IEEE Transactions on Smart Grid* 12.1 (2021), pp. 612–622 (cit. on p. 30).

[133] D. Choeum and D.-H. Choi. "OLTC-Induced False Data Injection Attack on Volt/VAR Optimization in Distribution Systems". In: *IEEE Access* 7 (2019), pp. 34508–34520 (cit. on p. 30).

[134] N. Bhusal, M. Gautam, and M. Benidris. "Detection of Cyber Attacks on Voltage Regulation in Distribution Systems Using Machine Learning". In: *IEEE Access* 9 (2021), pp. 40402–40416 (cit. on p. 30).

[135] A. Sawas and H. E. Z. Farag. "Two-fold Intelligent Approach for Successful FDI Attack on Power Systems State Estimation". In: *2018 IEEE Electrical Power and Energy Conference (EPEC)*. Oct. 2018, pp. 1–6 (cit. on p. 31).

[136] A. Abur and A. G. Exposito. *Power System State Estimation: Theory and Implementation*. CRC press, 2004 (cit. on pp. 35, 36).

[137] M. Ozay et al. "Sparse attack construction and state estimation in the smart grid: Centralized and distributed models". In: *IEEE Journal on Selected Areas in Communications* 31.7 (2013), pp. 1306–1318 (cit. on p. 37).

[138] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas. "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education". In: *IEEE Transactions on power systems* 26.1 (2010), pp. 12–19 (cit. on p. 41).

[139] A. Sawas et al. "Comparative Time-of-Use and wholesale electricity price-based scheduling in embedded power and natural gas distribution grids penetrated with large renewable generation". In: *Electric Power Systems Research* 177 (Dec. 2019), p. 105975 (cit. on p. 48).

[140] A. Sawas and H. E. Farag. "Optimal Sizing of Power–to–Gas Units toward Elevated Renewable Power Penetration". In: *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*. 2019, pp. 1–4 (cit. on p. 48).

[141] S. Mokhatab, W. A. Poe, and J. Y. Mak. "Chapter 11 - Natural Gas Compression". In: *Handbook of Natural Gas Transmission and Processing (Third Edition)*. Ed. by S. Mokhatab, W. A. Poe, and J. Y. Mak. Third Edition. Boston: Gulf Professional Publishing, 2015, pp. 349–381. ISBN: 978-0-12-801499-8 (cit. on p. 54).

[142] H. Bakhtiari and R. A. Naghizadeh. "Multi-criteria optimal sizing of hybrid renewable energy systems including wind, photovoltaic, battery, and hydrogen storage with ϵ-constraint method". In: *IET Renewable Power Generation* 12.8 (2018), pp. 883–892 (cit. on p. 57).

[143] P. M. de Quevedo, G. Muñoz-Delgado, and J. Contreras. "Impact of Electric Vehicles on the Expansion Planning of Distribution Systems considering Renewable Energy, Storage and Charging Stations". In: *IEEE Transactions on Smart Grid* (2018), pp. 1–1 (cit. on p. 57).

[144] M. Yan et al. "Coordinated Regional-District Operation of Integrated Energy Systems for Resilience Enhancement in Natural Disasters". In: *IEEE Transactions on Smart Grid* (2018), pp. 1–1 (cit. on p. 57).

[145] E. Mahboubi-Moghaddam et al. "Interactive Robust Model for Energy Service Providers Integrating Demand Response Programs in Wholesale Markets". In: *IEEE Transactions on Smart Grid* 9.4 (July 2018), pp. 2681–2690 (cit. on p. 57).

[146] Q. Zeng et al. "A multistage coordinative optimization for sitting and sizing P2G plants in an integrated electricity and natural gas system". In: *2016 IEEE International Energy Conference (ENERGYCON)*. Apr. 2016, pp. 1–6 (cit. on p. 58).

[147] A. Martinez-Mares and C. R. Fuerte-Esquivel. "A Unified Gas and Power Flow Analysis in Natural Gas and Electricity Coupled Networks". In: *IEEE Transactions on Power Systems* 27.4 (Nov. 2012), pp. 2156–2166 (cit. on pp. 59, 88).

[148] P. Grünewald, E. McKenna, and M. Thomson. "Keep it simple: time-of-use tariffs in high-wind scenarios". In: *IET Renewable Power Generation* 9.2 (2015), pp. 176–183 (cit. on p. 63).

[149] M. S. Ahmed, F. e. Bendary, and H. M. M. Moustafa. "Comparative study between: time of use and real-time pricing using fuzzy technique". In: *CIRED - Open Access Proceedings Journal* 2017.1 (2017), pp. 2641–2644 (cit. on p. 63).

[150] S. Nojavan, B. Mohammadi-Ivatloo, and K. Zare. "Optimal bidding strategy of electricity retailers using robust optimisation approach considering time-of-use rate demand response programs under market price uncertainties". In: *IET Generation, Transmission Distribution* 9.4 (2015), pp. 328–338 (cit. on p. 63).

[151] V. A. Evangelopoulos and P. S. Georgilakis. "Optimal distributed generation placement under uncertainties based on point estimate method embedded genetic algorithm". In: *IET Generation, Transmission Distribution* 8.3 (Mar. 2014), pp. 389–400 (cit. on p. 64).

[152] H. Liu et al. "Probabilistic load flow analysis of active distribution network adopting improved sequence operation methodology". In: *IET Generation, Transmission Distribution* 11.9 (2017), pp. 2147–2153 (cit. on p. 64).

[153] The Department of Energy Hydrogen and Fuel Cells Program Plan. *An Integrated Strategic Plan for the Research, Development, and Demonstration of Hydrogen and Fuel Cell Technologies*. Tech. rep. US Department of Energy), 2011 (cit. on p. 64).

[154] V. C. Gungor et al. "Smart Grid Technologies: Communication Technologies and Standards". In: *IEEE Transactions on Industrial Informatics* 7.4 (2011), pp. 529–539 (cit. on p. 78).

[155] N. S. Malik, R. Collins, and M. Vamburkar. *Cyber-attack Pings Data Systems of At Least Four Gas Networks*. Apr. 2018. URL: https://www.bloomberg.com/news/articles/2018-04-03/day-after-cyber-attack-a-third-gas-pipeline-data-system-shuts (visited on 08/2019) (cit. on p. 78).

[156] D. Batz et al. *Roadmap to achieve energy delivery systems cybersecurity*. Tech. rep. Cyber Security R&D Center, Menlo Park, CA: Department of Homeland Security, 2011 (cit. on p. 78).

[157] C.-C. Sun, A. Hahn, and C.-C. Liu. “Cyber security of a power grid: State-of-the-art”. In: *International Journal of Electrical Power & Energy Systems* 99 (2018), pp. 45–56 (cit. on p. 78).

[158] M. Shahidehpour and Y. Wang. “Appendix C: IEEE30 Bus System Data”. In: *Communication and Control in Electric Power Systems: Applications of Parallel and Distributed Processing*. 2003, pp. 493–495 (cit. on p. 88).

[159] W. R. Lacerda Junior et al. “Control of Hysteretic Systems Through an Analytical Inverse Compensation Based on a NARX Model”. In: *IEEE Access* 7 (2019), pp. 98228–98237 (cit. on p. 95).

[160] I. Zografopoulos et al. “Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies”. In: *IEEE Access* 9 (2021), pp. 29775–29818 (cit. on p. 104).

[161] U.S. Department of Energy. *Programmable Thermostats* (cit. on p. 111).

[162] U.S. Department of Energy. *Refrigerator Freezer Use and Temperature Tips* (cit. on p. 111).

[163] H. E. Z. Farag and E. F. El-Saadany. “A Novel Cooperative Protocol for Distributed Voltage Control in Active Distribution Systems”. In: *IEEE Transactions on Power Systems* 28.2 (2013), pp. 1645–1656 (cit. on p. 113).

[164] IEEE Standard. “IEEE Standard Requirements, Terminology, and Test Code for Step-Voltage Regulators”. In: *IEEE Std C57.15-2009 (Revision of IEEE Std C57.15-1999)* (2009), pp. 1–103 (cit. on p. 114).

[165] H. Gunduz and D. Jayaweera. “Modern power system reliability assessment with cyber-intrusion on heat pump systems”. In: *IET Smart Grid* 3.5 (2020), pp. 561–571 (cit. on p. 120).

[166] S. Hochreiter and J. Schmidhuber. “Long Short-Term Memory”. In: *Neural Computation* 9.8 (1997), pp. 1735–1780 (cit. on p. 120).

[167] Y. Goude, R. Nedellec, and N. Kong. “Local Short and Middle Term Electricity Load Forecasting With Semi-Parametric Additive Models”. In: *IEEE Transactions on Smart Grid* 5.1 (2014), pp. 440–446 (cit. on p. 122).

[168] B. L. Bowerman, R. T. O’Connell, and A. B. Koehler. *Forecasting, time series, and regression: an applied approach*. Vol. 4. South-Western Pub, 2005 (cit. on p. 124).

[169] A. Agresti and B. A. Coull. “Approximate is better than “exact” for interval estimation of binomial proportions”. In: *The American Statistician* 52.2 (1998), pp. 119–126 (cit. on p. 125).

[170] D. P. Chassin, K. Schneider, and C. Gerkensmeyer. “GridLAB-D: An open-source power systems modeling and simulation environment”. In: *2008 IEEE/PES Transmission and Distribution Conference and Exposition*. 2008, pp. 1–5 (cit. on p. 125).

[171] M. Z. Gunduz and R. Das. “Cyber-security on smart grid: Threats and potential solutions”. In: *Computer Networks* 169 (2020), p. 107094. ISSN: 1389-1286 (cit. on p. 135).

[172] A. Sawas, H. Khani, and H. E. Z. Farag. “On the Resiliency of Power and Gas Integration Resources Against Cyber Attacks”. In: *IEEE Transactions on Industrial Informatics* 17.5 (2021), pp. 3099–3110.

Appendix A

List of Publications

1. **A. Sawas** and H. E. Z. Farag. "Two-fold Intelligent Approach for Successful FDI Attack on Power Systems State Estimation". In: 2018 IEEE Electrical Power and Energy Conference (EPEC). Oct. 2018, pp. 1–6.
2. **A. Sawas**, H. Khani, N. El-Taweel, and H. E.Z. Farag, "Comparative Time-of-Use and wholesale electricity price-based scheduling in embedded power and natural gas distribution grids penetrated with large renewable generation". In: Electric Power Systems Research 177 (Dec. 2019), p. 105975.
3. **A. Sawas** and H. E. Farag. "Optimal Sizing of Power–to–Gas Units toward Elevated Renewable Power Penetration". In: 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE). 2019, pp. 1–4.
4. **A. Sawas**, H. Khani, and H. E. Z. Farag. "On the Resiliency of Power and Gas Integration Resources Against Cyber Attacks". In: IEEE Transactions on Industrial Informatics 17.5 (2021), pp. 3099–3110.
5. **A. Sawas** and H. E. Z. Farag. "Real-Time Detection of Surreptitious IoT-Based Cyber Attacks in Power Distribution Systems: A Novel Anomaly Prediction Approach". Submitted for review to Electric Power System Research Journal, Aug 2022.

Appendix B

Attributions

Clips used in Figure 1.1 are downloaded from "www.freepik.com" with permission to use under Free License.