Detection of Cyber Attacks in Power Distribution

Energy Management Systems

by

Vaithinathan Ravi

A Thesis Presented in Partial Fulfillment
of the Requirements for the Degree
Master of Science

Approved November 2014 by the
Graduate Supervisory Committee:

Gerald Heydt, Chair
George Karady
Lalitha Sankar

ARIZONA STATE UNIVERSITY

December 2014

ABSTRACT

The objective of this thesis is to detect certain cyber attacks in a power distribution energy management system in a Smart Grid infrastructure. In the Smart Grid, signals are sent between the distribution operator and the customer on a real-time basis. Signals are used for automated energy management, protection and energy metering. This thesis aims at making use of various signals in the system to detect cyber attacks. The focus of the thesis is on a cyber attack that changes the parameters of the energy management system. The attacks considered change the set points, thresholds for energy management decisions, signal multipliers, and other digitally stored parameters that ultimately determine the transfer functions of the components. Since the distribution energy management system is assumed to be in a Smart Grid infrastructure, customer demand is elastic to the price of energy. The energy pricing is represented by a distribution locational marginal price. A closed loop control system is utilized as representative of the energy management system. Each element of the system is represented by a linear transfer function. Studies are done via simulations and these simulations are performed in Matlab SimuLink. The analytical calculations are done using Matlab.

Signals from the system are used to obtain the frequency response of the component transfer functions. The magnitude and phase angle of the transfer functions are obtained using the fast Fourier transform. The transfer function phase angles of base cases (no attack) are stored and are compared with the phase angles calculated at regular time intervals. If the difference in the phase characteristics is greater than a set threshold, an alarm is issued indicating the detection of a cyber attack.

The developed algorithm is designed for use in the envisioned Future Renewable Electric Energy Delivery and Management (FREEDM) system. Examples are shown for the noise free and noisy cases.

I would like to dedicate this thesis to my parents, Ravi Vaithinathan and Mangalam Ravi, who encouraged me to pursue my Master's degree with thesis and showed support when I was in need. I also dedicate this thesis to all my well-wishers and friends who have believed in me throughout my journey as a Master's student. Finally, I would like to thank God for all that I have been given in life. I hope this thesis is just the start for many more things to come in my life.

ACKNOWLEDGEMENTS

I would like to thank my advisor and chair Dr. Gerald T. Heydt for the opportunity to work with him. I will forever be grateful to him for the guidance and encouragement provided by him. The research opportunity has taught me a lot of things that none of the courses might be able to and I am thankful for that. I also thank Dr. George Karady and Dr. Lalitha Sankar for their time and effort in being a part of my supervisory committee.

Finding for this research was provided by the Future Renewable Electric Energy Delivery and Management (FREEDM) center, founded by National Science Foundation (NSF).

Finally, I would like to thank Arizona State University for providing the perfect institution for my Master's degree and for making my journey a memorable one.

TABLE OF CONTENTS

Page

CHAPTER Page

LIST OF FIGURES

Figure Page

LIST OF TABLES

Table Page

NOMENCLATURE

a	Point of signal extraction in the test bed
$A_{1\times N}$	Array containing 1 row and N columns representing the input signal A(s) in time domain
A(s)	Arbitrary input to a feedback control system in *s*-domain
AMI	Automated Metering Infrastructure
b	Point of signal extraction in the test bed
$B_{1\times N}$	Array containing representing the output signal B(s) in time domain
B(s)	Output of a feedback control system in *s*-domain
c	Point of signal extraction in the test bed
$c(t)$	Input command to a system in time domain
$C(j\omega)$	Input to a closed loop system written as a function of frequency
C(s)	Input to a closed loop system in *s*-domain
d	Point of signal extraction in the test bed
D	Demand
DAM	Data Association Mining
DC	At zero frequency
DLMP	Distribution Locational Marginal Price
e	Point of signal extraction in the test bed
e(t)	Signal including effect of Price modifier block
f	Frequency
$f(t)$	Function in time domain

$F(s)$	Laplace transform of $f(t)$ in *s*-domain
FFT	Fast Fourier Transform
$FFT\_A_{1\times N}$	Array containing Fast Fourier transform of input array *A*
$FFT\_B_{1\times N}$	Array containing Fast Fourier transform of output array *B*
FRA	Frequency Response Analysis
FREEDM	Future Renewable Electric Energy Distribution and Management Center
FRTU	Feeder Remote Terminal Units
$G(j\omega)$	Transfer function block in a closed loop system represented as a function of frequency
$G(s)$	Transfer function block in a closed loop system in *s*-domain
$h(t)$	Impulse response of H(s)
$H_{k=1}^{N}$	Array storing the ratio of $FFT\_B_{1\times N}$ divided by $FFT\_A_{1\times N}$
$H(j\omega)$	Transfer function block in a closed loop system represented as a function of frequency
$H(s)$	Transfer function block in the feedback loop of a closed loop system in *s*-domain
$H_S(s)$	Transfer function representing block *S* in the test bed
$H_S'(s)$	Transfer function representing block *S* after a cyber attack
$H_{calc}(j\omega)$	Transfer function between a set of points in the calculated system
$H\_mag_{k=1}^{N}$	Array representing magnitude of complex array $H_{k=1}^{N}$

$H\_phase_{k=1}^{N}$	Array representing phase angle of complex array $H_{k=1}^{N}$
IAE	Integral Absolute Error
IHD	In-Home Displays
ISE	Integral Square Error
j	Iteration index
k	Arbitrary node in a power system distribution network, Iteration index
$K(s)$	Controller in a closed loop feedback control system
$ku(t)$	Representation of step input of magnitude k as a function of time
LMP	Locational Marginal Price
LTI	Linear Time Invariant
$\max\_ang\_diff_{1\times 6}$	Array containing maximum phase angle differences between base case and the calculated case
MCC	Marginal Congestion Cost
MEC	Marginal Energy Cost
MLC	Marginal Loss Cost
n	Arbitrary integer
NSF	National Science Foundation
OPF	Optimal Power Flow
P	DLMP input pricing signal to the test bed
Q	Transfer function block representing a part of the demand-price relation used in the test bed

Q'	Transfer function block representing a part of the demand-price relation used in the test bed
r	Point of signal extraction in the test bed
$r(t)$	Output of a system at time t
$r_d(t)$	Desired output of a system at time t
R	Transfer function block in the test bed representing system dynamics
$R(j\omega)$	Output of a closed loop system written as a function of frequency
$R(s)$	Output of a closed loop system in s-domain
RMS	Root Mean Square
$RMS_{\max}$	Maximum permissible RMS error function
s	Laplace domain variable
S	Transfer function block in the test bed representing sensor dynamics
t	Time
T	Time, Transfer function block in the test bed representing the price controller
$TF_{c\to a}$	Transfer function between c and a
$TF_{c\to b}$	Transfer function between c and b
$TF_{c\to d}$	Transfer function between c and d
$TF_{c\to r}$	Transfer function between c and r
$TF_{e\to d}$	Transfer function between e and d
$TF_{p\to q}$	Transfer function between p and q

$TF_{r \to b}$	Transfer function between *r* and *b*
$T_{CR}(j\omega)$	Transfer function between C and R in a closed loop system as a function of frequency
WND	Weighted Normalized Difference
$x_1(t)$	Sample input signal to a linear system
$x_2(t)$	Sample input signal to a linear system
$y(t)$	Output of a system in time domain
$y_1(t)$	Output of a linear system for an input $x_1(t)$
$y_2(t)$	Output of a linear system for an input $x_2(t)$
Y(s)	Output of a closed loop feedback system in *s*-domain
α_1	Scalar coefficient
α_2	Scalar coefficient
Δ	Phase angle difference between base case and calculated case
ΔQ	Change in block *Q*
$\Delta Q'$	Change in block *Q'*
ΔR	Change in block *R*
ΔS	Change in block *S*
Δt	Small time step
ΔT	Change in block *T*
$\varepsilon(t)$	Error function at time *t*
τ	Time lag

ω	Frequency (in rad/s)
ζ	Array used to display if there is a cyber attack in the system or not
$\mathfrak{I}$	Flag matrix

CHAPTER 1

ENERGY AND POWER MANAGEMENT IN DISTRIBUTION SYSTEMS

1.1 Objectives of this Research

The objective of this thesis is to detect cyber attacks in a closed loop distribution energy management system in a Smart Grid infrastructure. In the Smart Grid, signals are sent between the distribution operator and customer on a real-time basis. Also, signals are used for automated energy management, protection and energy metering. There are different possible reasons for wrong information to be fed back. The contents of this thesis focus on the detection of cyber attacks. These are the reasons for incorrect data to be sent to the distribution operator or the automated energy management system. Models are created in Matlab Simulink and the systems are analyzed in the *s*-domain. The proposed method utilizes a phase change detection property of energy management component transfer functions.

1.2 The FREEDM System

The Future Renewable Electric Energy Delivery and Management (FREEDM) system was established by the National Science Foundation (NSF) in 2008. Objective of the FREEDM center is to develop innovative technology for the power industry, improving energy reliability and security [1]. The universities participating in the FREEDM systems include North Carolina State University, Arizona State University, Florida Agricultural and Mechanical University, Missouri University of Science and Technology, ETH Zurich and Florida State University [2].

The envisioned FREEDM system aims at making changes to the contemporary power grid network. The basic concept is to replace the traditional 60 Hz transformers with solid state transformers and the mechanical switches with solid state based protection devices [3]-[10].

This thesis contributes to the FREEDM systems research by developing a method of detecting cyber attack in a distribution energy management system in a Smart Grid infrastructure.

1.3 Distribution Energy Management System in a Smart Grid Infrastructure

The distribution energy management system in a Smart Grid infrastructure is represented in a closed loop control system structure. There are various elements in the system, which are all represented by control system blocks. Each of these elements and blocks is explained in the sections that follow. The transfer functions representing the blocks are chosen carefully and the whole system is designed such that,

- the system in open loop state is stable i.e., the open loop transfer function of the system contains all the poles on the left half plane.
- the system in closed loop state is stable i.e., the closed loop transfer function of the system contains all the poles on the left half plane.

The schematic representation of the distribution energy management system in a Smart Grid infrastructure is shown in Figure (1.1). The concepts implemented are explained in the sections that follow.

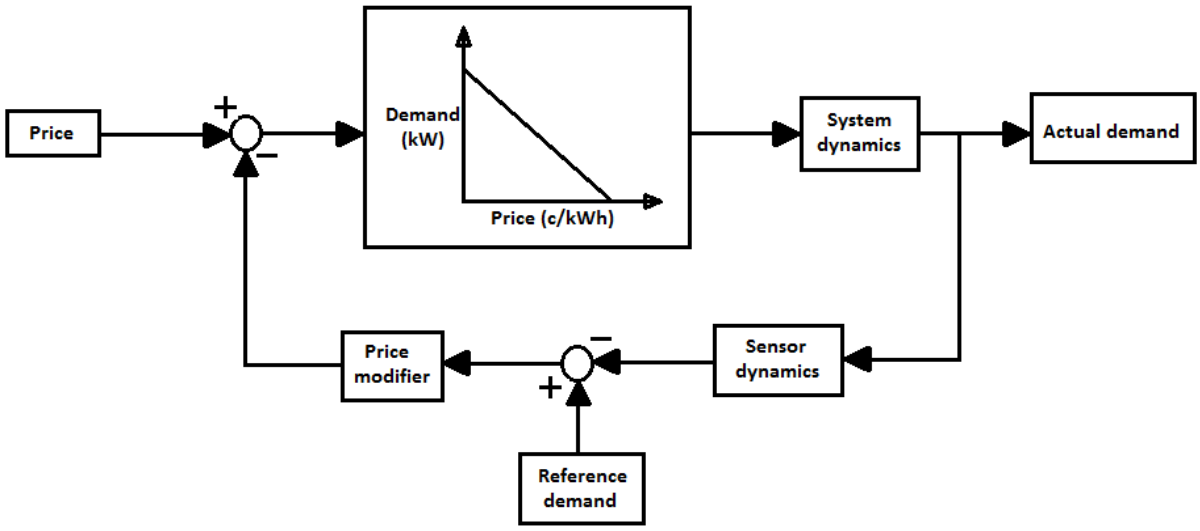

Figure (1.1) Schematic of Distribution Energy Management System in a Smart Grid

1.4 Linear Time Invariant Systems

The system in consideration in this thesis is a Linear Time Invariant (LTI) system. A system is said to be an LTI system if the system's output waveform is the same as long as the initial state and the input to the system are the same, irrespective of the time that they are applied at [11].

In order to make understanding better, the concept of linearity and time invariance are explained separately by the author in [12].

- Linearity - Let $x_1(t)$ and $x_2(t)$ be any two signals. Let the output of a system to $x_1(t)$ be $y_1(t)$ and the output of the same system to $x_2(t)$ be $y_2(t)$. If, for an input of $\alpha_1 x_1(t) + \alpha_2 x_2(t)$, the output of the system is $\alpha_1 y_1(t) + \alpha_2 y_2(t)$ at all times, it implies that the system is linear. The foregoing definition assumes that $y(t) = 0$ when $x(t) = 0$ If this is not the case, it is necessary to account for the component of $y(t)$ due to input $x(t) = 0$.

- Time invariance – A system is said to be time invariant if, when $y(t)$ is the output for an input $x(t)$, then for any τ, $y(t-\tau)$ is the output for an input $x(t-\tau)$.

When a system has both the properties mentioned above, it is said to be an LTI system.

1.5 Frequency Domain Analysis of Control Systems

In practice, the performance of a feedback control system is preferably measured by its time domain response characteristics. In contrast, frequency response is of more importance in cases where the signals are mostly sinusoidal or periodic in nature. For this purpose, control system analysis and design are conducted in the frequency domain. This is used as a convenient vehicle towards the same objectives as with time domain methods [13]. Transfer function is used to characterize an LTI system. In general, the relationship between input and output of a system is given by differential equations, when input and output are functions of time [14]. Studying systems using differential equations gets tougher as the systems get more complex. For this purpose, the differential equations are transformed into a convenient form by using the *Laplace transform*, a function of frequency [25]. Conversion of time domain function to the *s*-domain, $f(t) \leftrightarrow F(s)$, is given as,

$$F(s) = \int_0^\infty f(t)e^{-st}dt. \tag{1.1}$$

A generic feedback control system is shown in Figure (1.2). In *s*-domain, the input-output relation is described as,

$$T_{CR}(s) = \frac{R(s)}{C(s)} = \frac{G(s)}{1+G(s)H(s)}. \tag{1.2}$$

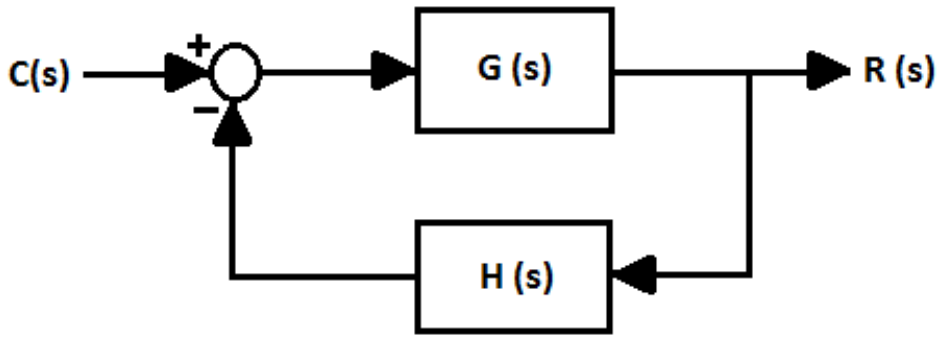

Figure (1.2) Simple Feedback System

Under sinusoidal steady state, $s = j\omega$. On substituting,

$$T_{CR}(j\omega) = \frac{R(j\omega)}{C(j\omega)} = \frac{G(j\omega)}{1 + G(j\omega)H(j\omega)}. \tag{1.3}$$

Note that $T_{CR}(j\omega)$ is a complex function of frequency, ω. Hence, T_{CR} can be expressed as a function of magnitude and phase angle,

$$T_{CR}(j\omega) = |T_{CR}(j\omega)| \angle T_{CR}(j\omega). \tag{1.4}$$

Magnitude and phase angle plots are obtained when the magnitude and phase angles are plotted as a function of frequency, against frequency, ω.

1.6 Need for Feedback Control

A control system is an interconnection of subsystems consisting of sensor, controller and actuator. When the system operates in open loop, it is highly sensitive to uncertainty i.e., uncertainty associated with desired outputs, disturbances and the system itself. To account for this uncertainty, a closed loop system is used i.e., a feedback loop is implemented, which reduces the

sensitivity to a large extent. According to [16], feedback refers to the use of sensor provided information by a controller for the purpose of decision making with the goal of achieving desirable closed loop characteristics.

In this thesis, the system under consideration is that of a distribution energy management system which decides the load at the consumer side depending on the pricing signal from the distribution operator end. Since the price of energy does not remain constant, an open loop system may not function very well. For this purpose, a feedback control system is proposed, as shown in Figure (1.1). The feedback loop has a 'Price modifier' block, which uses the difference between the actual load on the consumer side and the load level set by the distribution operator to modify the signal going to the customer, thereby controlling customer load.

1.7 The Demand-Price Relation

Economic theory states that there is a negative relation between the demand for a particular commodity and its price. It states that the demand for electricity should decrease when there is a hike in price for an additional unit of energy. When it comes to electricity market, the relationship between energy demand and the price of energy is less elastic [17]. This is because the consumer does not have access to the price of energy on a real-time basis. Only at the end of each month the users get to know their consumption, in units of currency and energy.

It is known that there can be energy saving of up to 20 percent if the customer are made known of the price that they are paying for electricity at any given point of time. One such method of achieving this is by making use of devices like In-Home Displays (IHD), where the consumers are provided with direct feedback of real-time energy consumption information, in units of energy and currency [18]. Another method is by making use of Automated Metering Infrastructure (AMI)

technology which uses an "agent-based model to demonstrate and quantify the economic impact of price elasticity of demand in electricity markets when consumers are well equipped with Smart Grid technologies to increase their awareness of responsiveness of demand" [19]. Research has been done in the field using Data Association Mining (DAM) algorithms which makes use of a multi-input multi-output forecasting engine to make price and demand predictions so that consumers can react to electricity prices [20].

Studies have been conducted on the extent to which consumers respond to a variation in price [21]. It has been concluded that consumer behavior can be modeled using a matrix of self and cross elasticities to get to an overall approximate relation between the demand and price in a Smart Grid infrastructure. A typical elastic and inelastic relationship between demand and the price of electricity is depicted in Figure (1.3).

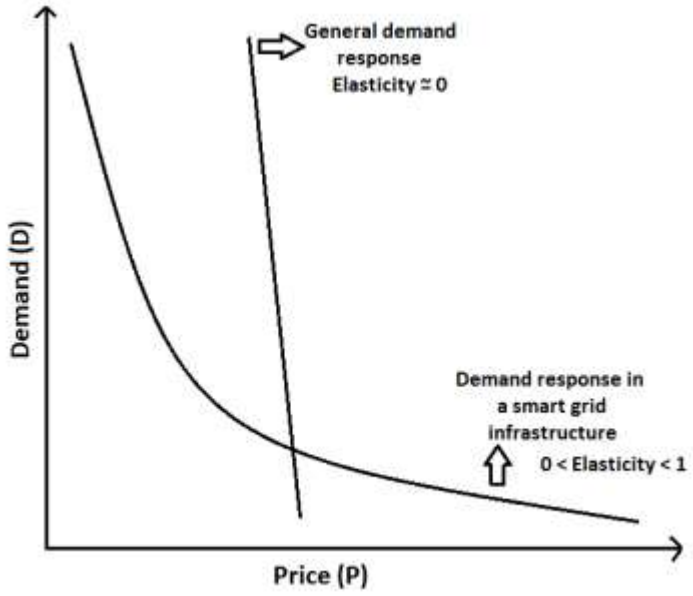

Figure (1.3) Typical Elastic and Inelastic Demand-Price Relationship

Any one of the above mentioned techniques is used in a Smart Grid, making the relationship between demand and price of electricity elastic. A suitable demand-price algebraic relation is used for studies in this work. For the sake of simplicity, demand is taken to have a linear relationship with price. The control block representing the demand-price relation is shown in Figure (1.4).

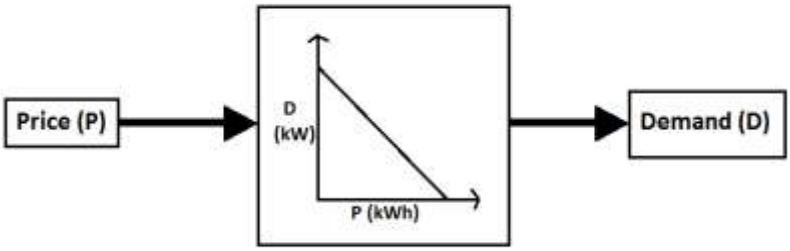

Figure (1.4) Open Loop Control Structure of a Controlled Smart Grid Distribution System

1.8 Integral Absolute Error

A common and easy method of assessing the performance of a given system uses the Integral Square Error (ISE). ISE was suggested by James, Nichols and Philips [22]. For any input, a convenient integral function could be designed to obtain an index of performance. An example is the integral function of error. In [22], an *RMS error* function was given as,

$$RMS^2 = \lim_{T\to\infty} \frac{1}{T} \int_0^T \varepsilon^2(t)dt\,. \tag{1.5}$$

where $\varepsilon(t)$ is the error value at any given time *t*. $\varepsilon(t)$ is a generic error function such as the difference between a given output *r(t)* and the desired output $r_d(t)$. If the maximum permissible *RMS error* function is specified, a feedback control may be designed such that,

$$RMS \le RMS_{\max}. \tag{1.6}$$

This *RMS error* criterion has been used in many designs. The reason for its extensive use is its mathematical convenience and the fact that the method weighs the extent of undesirability of an error as the error increases. The ISE signal is used in control theory for the design of robust feedback controls.

According to [23], the *RMS error* method is used to design various parameters of a control system such as component block gains, loop gains at a given frequency, and other component specific parameters. It is possible to do this for linear systems or nonlinear systems. Newton, Gould and Kaiser introduced this procedure to control engineering practice [24]. For step inputs, they used the ISE method, described below, and for statistical type inputs, they made use of the conventional *RMS error* criterion.

According to the authors of [25], an analytical method for the ISE criterion is much better than a numerical method. ISE is analytically formulated for linear continuous feedback control systems when the system is asymptotically stable in its closed loop and the error function is proper at all times. A typical feedback control system is shown in Figure (1.5).

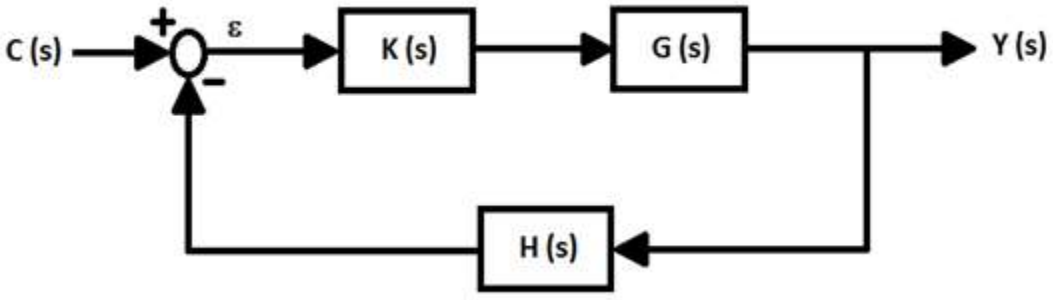

Figure (1.5) Typical Closed Loop Feedback Control System

In Figure (1.5), ε is the error value. The figure represents a simple feedback controller in which the time domain error function $\varepsilon(t)$ is given by,

$$\varepsilon(t) = c(t) - h(t) * y(t) . \tag{1.7}$$

where *c(t)* is the input command and *y(t)* is the output. The notation (*) denotes convolution. The feedback gain is *H(s)* whose impulse response is given by *h(t).* The ISE function of the system is given by,

$$ISE = \int_0^\infty \varepsilon^2(t)dt. \tag{1.8}$$

An alternative index of performance for this particular case is the Integral Absolute Error (IAE),

$$IAE = \int_0^\infty | \varepsilon(t) | dt . \tag{1.9}$$

where $\varepsilon(t)$ is a generic error function such as the difference between a given output *r(t)* and a desired output $r_d(t)$.

In (1.9), the absolute error at a given time, *t,* would be the absolute difference between the actual value of the output and the desired output value, if *H(s)* is unity. If $\varepsilon(t)$ is an error power level (e.g., the difference between a desired load level and an actual load level), then the IAE is an error energy.

1.9 Cybertampering

Cybertampering refers to a disruption in accurate measurement of electricity usage by customers. Feeding in false electricity usage data to the distribution operators by the customers in order to reduce their electricity bill is a type of cyber attack. There are a number of techniques

adopted by the customers to tamper the usage data that is fed back. In [26], the authors speak about various methods of energy theft, which are essentially methods of tampering with the electricity usage data that is fed back from the customer side. A comparative study of the extent of energy theft in 102 different countries was done for the years 1980 and 2000 by the author in [27]. It was seen that the extent of theft increased, resulting in higher electricity prices for the customers. This is turning out to be a critical issue where a part of the public is taking advantage of the innocent rest. This calls for better and effective methods of identifying energy theft in a system. Attempts have also been made to use distribution system state estimation to detect bad measurements from AMI real-time data [28]-[30]. The applications to distribution systems were limited due to the large number of state variables and small number of redundancies.

The authors of [26] state that energy theft includes "using unregistered electrical appliances, using alternate neutral lines, tampering with meters/terminals, sabotaging control wires, using magnets to decelerate the spinning discs for recording the energy consumption and tapping off of a neighbor." The authors have addressed a mechanism to counter such tampering techniques. The mechanism proposed uses an online data validation framework, which checks if the measurements from the home energy meters match with the measurements obtained from verification points at different levels in the system (feeder level, subsystem level, customer level). At the feeder level, the availability and integrity of the Feeder Remote Terminal Units (FRTU) is checked. This is achieved by analyzing the log information recorded by the FRTUs. An FRTU is deemed unreliable if malfunction events are observed from its log information.

At the second level, a value called *mismatch ratio* is calculated for all the subsystems. It indicates the level of inconsistency of the metering data. These values are allotted by performing

power flow at the subsystem level. There are a few disadvantages of adopting this algorithm, which are discussed in detail in a section later. Once the faulty subsystem is identified, a pattern recognition method is adopted to detect the customers that have been sending out faulty data.

According to the U.S Department of Energy, one of the main qualities of a Smart Grid is that, any problem in the grid element should be identified, isolated and corrected with no human intervention [31], [32]. The process of treating itself has been termed *self-healing*. Basically, self-healing is automation of power system control, monitoring and protection using advanced technology.

Though it is unknown, as to, how far the self-healing Smart Grid can be achieved in reality, striving towards this goal is only going to make things better from the cyber security point of view [33]. Authors of [33] see the need to categorize the various elements in a Smart Grid infrastructure, into *high risk*, *medium risk* and *low risk*, depending on the level of risk the element's failure would pose to the electrical grid. Control systems room and transmission are the only elements that pose high risk on failure. It is concluded in [33] that it is not only necessary to increase the security capabilities of the system, but it is also important to be able to independently validate the accuracy and reasonableness of commands from any distributed sensors. This is done by synthesizing the command from the distributed sensor and the control room operator and sending it forward to the next element only when the command signal is found to be genuine.

1.10 Organization of this Thesis

Chapter 1 has explained the fundamentals of the concepts that form the foundation of the work done in this thesis. The concepts include FREEDM system, distribution energy management

system, Smart Grid, price-demand relation, linearity, time invariance, cybersecurity, need for feedback control and integral absolute error as an index of performance. In Chapter 2, a test bed is designed to test the algorithm. The test bed is representative of a distribution energy management system. Each component in the test bed is explained and an appropriate transfer function is assigned to represent each of the components. Once the test bed is explained in detail, the algorithm developed to detect cyber attacks is explained.

Chapters 3 and 4 involve results of simulations conducted to test the validity of the algorithm developed. Chapter 3 deals with a noise free environment, whereas Chapter 4 has simulation results of the test bed in a noisy environment. Chapter 5 makes conclusions about the study done in this thesis and there are some recommendations on possible future work in the same field. The Appendix section contains Matlab codes that are used to implement the algorithm developed in this work.

CHAPTER 2

A THEORETICAL BASIS FOR CYBER ATTACKS DETECTION IN POWER DISTRIBUTION MANAGEMENT SYSTEMS

2.1 Model of a Distribution Energy Management System

The system under consideration in this thesis is assumed to be in a Smart Grid infrastructure. The main features adopted are:

- A pricing signal, called Distribution Locational Marginal Price (DLMP), is used as the control signal to control the demand level at the customer end.
- Signals are constantly fed back to the automated energy management system.
- Customer demand is elastic to variations in the DLMP signal.

A schematic representation of the system is shown in Figure (1.1). A test bed is created for testing and running simulations. It is shown in Figure (2.1). Each block represented in the test bed (*P*, *Q*, *Q'*, *R*, *S*, *T*) will be explained in the upcoming sections.

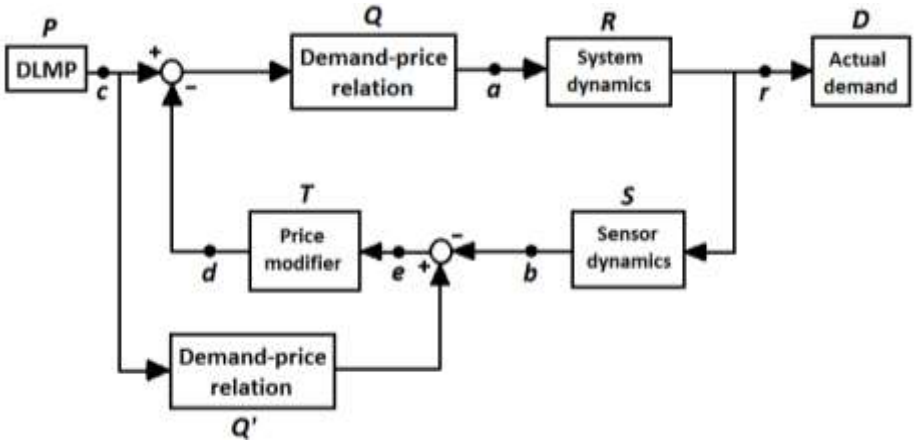

Figure (2.1) Schematic of Test Bed Created to Study a Distribution Energy Management System

Each node in a system has its own LMP, which is essentially the price of an additional unit of energy. In [36], LMP is defined as "the marginal cost supplying, at least, the next increment of electric demand at a specific location (node) on the electric power network, taking into account both supply (generation/import) bids and demand (load/export) offers and the physical aspects of the transmission system including transmission and other operational constraints." A lot of research has been done in the field of LMPs and their importance [37]-[39].

However, LMP would not be sufficient for the control of loads in the Smart Grid. Methods were developed to set something called a *spot price* [40]. The concept of *spot pricing* was viewed to be different from conventional pricing and control methods. The authors of [40] feel that the customer should be penalized for contributing to the system peak, not for their own peak. Spot pricing takes both, supply and demand factors, into consideration.

The concept of LMP was modified at the distribution level for use in the Smart Grid applications. This was termed as the Distribution Locational Marginal Price (DLMP) signal. A number of formulations of this pricing signal have been done [41]. According to the authors of [42] the DLMP is a much more accurate pricing of an additional unit of energy at the distribution level. The reason given was that DLMP includes Marginal Energy Cost (MEC), Marginal Loss Cost (MLC) and Marginal Congestion Cost (MCC).

Further, the existing flat-rate retail system, defined by LMP at the nodes, causes market inefficiency [43]. Various techniques were developed for the calculation of LMP in distribution systems (e.g., a distribution LMP or DLMP), one of which was the use of quadratic programming and the Karush-Kuhn-Tucker method [44]. Another method takes into consideration demand response to calculate DLMP [45]. The cited method involves using LMP as the starting point for the

formulation of the DLMP. Price responsive load Optimal Power Flow (OPF) was used to build the constraints and solve for the DLMP.

In the tests conducted, the input price signal to the system is assumed to be the DLMP at the particular customer service entrance. Since, this thesis deals with systems at the distribution level, representation of the input pricing signal as a DLMP signal would be appropriate. The customer in the test bed is assumed to be a residential customer. The DLMP signal could take values in the range of 0.01 \$/kWh – 0.25 \$/kWh. For testing purposes in this thesis, the change in DLMP is represented as a step input $ku(t)$ of amplitude k plus a sinusoidal input of amplitude 0.005 and frequency 1.0 rad/s. In some tests, noise is added to simulate the usual variation of DLMP with time. This particular test signal is used to excite dynamics in the energy management system and to obtain an output signal (i.e., the controlled load) that is suitable for signal analysis.

2.3 Demand-Price Relation

The demand-price relation, in the case of electricity, is pretty inelastic. This is because the customers are not aware of the price being paid for a unit of energy in real time. In a Smart Grid infrastructure, customers are made aware of the real time pricing of electricity through Smart Meters, AMI technology and DAM algorithms. It could be concluded that consumer behavior can be modeled to get to an overall approximate relation between the demand and price in a Smart Grid infrastructure. Real-time pricing and billing monitors consumption in real time and bills immediately, giving consumers flexibility to track and pay for usage.

For testing purposes, demand is taken to be elastic to changes in input DLMP. For convenience the relation is considered to be linear. The demand (D) for a price level (P) is given by,

$$D = 10 - \frac{100}{3} P \,. \tag{2.1}$$

where the price (P) is in \$/kWh and demand (D) is in kW. Such a relation allows price to vary from 0 \$/kWh to 0.30 \$/kWh, although the DLMP pricing signal is taken to vary anywhere between 0.01 \$/kWh and 0.25 \$/kWh. The graphical representation of (2.1) is given in Figure (2.2).

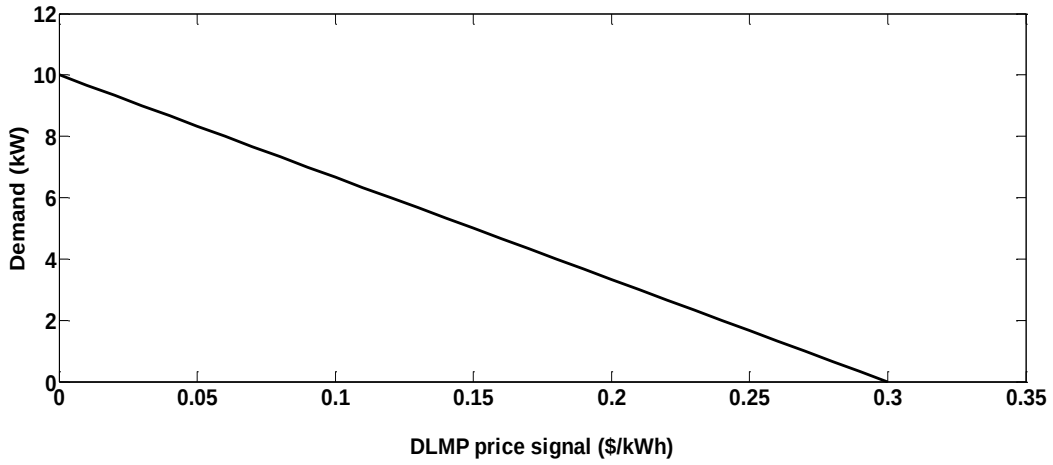

Figure (2.2) Demand-Price Relation Used in the Tests

2.4 System and Sensor Dynamics

The blocks *System dynamics* and *Sensor dynamics* in the test bed represent the fact that a system does not respond immediately to a given signal. The system takes its time to settle at the final state once it receives the signal. The signal that the test bed receives is that of a pricing signal. When price per unit of electricity changes, the system takes its time to settle at modified demand level. This is due to the *System dynamics* block. This block is designed in such a way that the system is very slow. This calls for a feedback loop, which makes the system comparatively faster. The comparison between open loop system and the closed loop system is done in one of following sections. Similarly, the *Sensor dynamics* block is used to represent the time delay associated with

the sensor signals. Signals detected by the sensor are not transmitted immediately. The sensor is taken to be faster than the system in its open loop. Both the blocks are represented by transfer functions in the test bed. The transfer functions used are,

$$System\ dynamics = \frac{0.04}{s + 0.04} \tag{2.2}$$

$$Sensor\ dynamics = \frac{10}{s + 10}. \tag{2.3}$$

These transfer functions are represented as "typical," but it is noted that if other transfer functions are used, the subsequent analysis procedure is still valid.

2.5 Test Bed

The different properties and blocks used in the test bed have been explained in Sections 2.1 – 2.4. The test bed is designed in SimuLink and is shown in Figure (2.3).

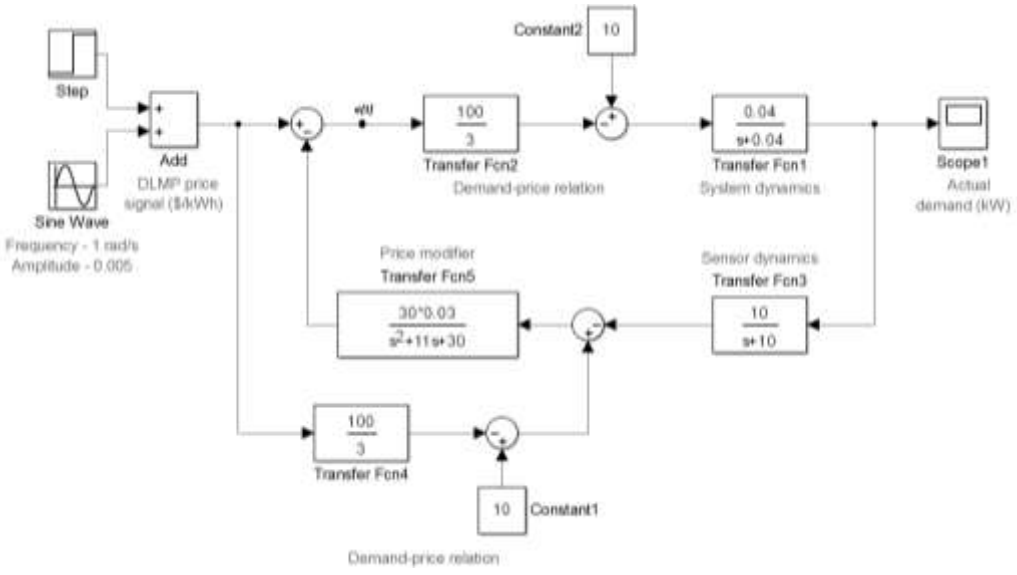

Figure (2.3) Energy Management Control System Test Bed Used in All Noise Free Test Cases

2.6 Price Modifier Block

As explained in Section 2.4, a feedback loop is used to make the system faster i.e., respond faster to changes in input signal. The actual demand at a given instant, *t*, is compared with the reference demand signal and the error is fed back through a *Price modifier* block. The function of the *Price modifier* block is to make the demand settle at the corresponding value faster. *Price modifier* block is represented by a transfer function, given as,

$$Price\ modifier = \frac{(30)(0.03)}{s^2 + 11s + 30}. \tag{2.4}$$

To illustrate the effect of having a feedback loop modifying certain control signals (e.g., the signal *e(t)* shown in Figure (2.3)), an example is shown. Initially the test bed has been functioning with an input price of 0.10 $/kWh. Correspondingly, the demand is at 6.667 kW. The price signal is now modified to 0.20 $/kWh and the response of the system in its open loop and closed loop are observed. The difference in system response is shown in Figure (2.4). Note that the integral of the demand power is *energy*. And therefore the area between the two curves shown in Figure (2.4) is the energy difference. In the example shown, the energy difference with and without feedback is approximately 112 kJ.

The DC gain of the *Price modifier* block is 0.03, which essentially means that in the steady state, there is a change of 0.03 $/kWh in the signal *e(t)* for a difference of 1 kW between the actual demand and the reference demand.

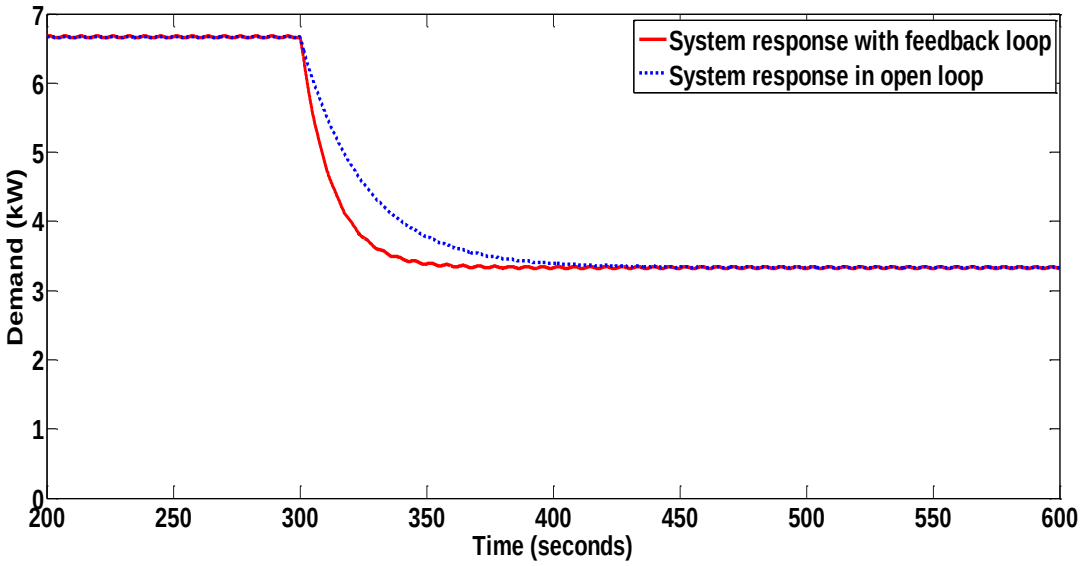

Figure (2.4) Comparison of Response (Controlled Load) of the Test Bed System in Open Loop and Closed Loop Configurations

2.7 Frequency Response Analysis

Signals from different points in the system are sent to the automated energy management system on a real-time basis. These signals can be used to check if the system has been compromised by performing Frequency Response Analysis (FRA). With all FRA techniques, one of the main limitations has been the lack of an objective to compare two different transfer functions. Different methodologies have been adopted in the past as an evaluating parameter. In [43], the authors evaluated the difference between two transfer functions by defining Weighted Normalized Difference (WND). Other evaluating parameters have also been used in the past [44]-[46]. In the tests conducted, the phase angles of the transfer functions will be compared with base case phase angles.

2.8 Transfer Function Estimation

The transfer function is obtained from the numerical signal values from the sensors in the system. The frequency response of the transfer function between two given points, *A* and *B*, can be obtained by performing Fast Fourier Transform (FFT). Note that *A* is the input signal and *B* is the output signal. Dividing the FFT of *B* array by the FFT of *A* array, term by term, gives the frequency response of the transfer function between *A* and *B*. To make understanding of this method better, a simple schematic representation is shown in Figure (2.5). This algorithm is implemented in Matlab where the term by term division is denoted by "./"

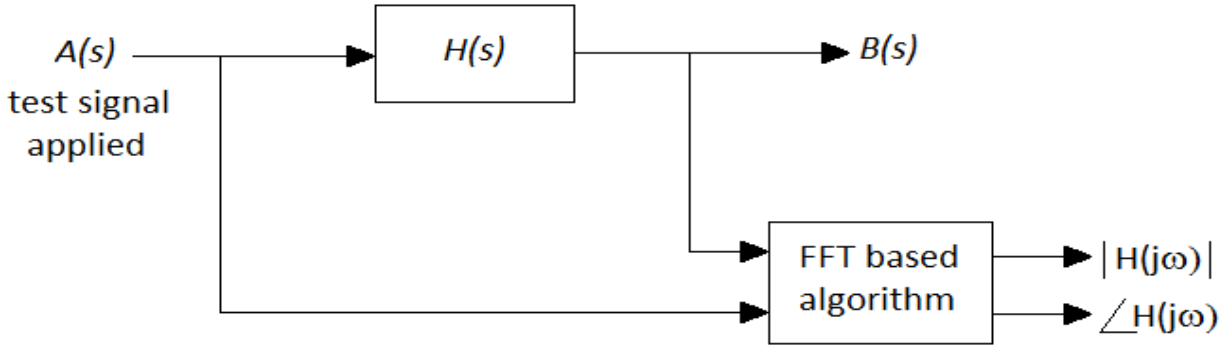

Figure (2.5) Example for Transfer Function Estimation Using the FFT

A and *B* are signals in time-domain, calculated at regular intervals, and are stored in an array of length *N*. The signals are sampled a regular time intervals of Δt. The transfer function between the points *A* and *B* is given by $H(s)$. The arrays $A_{1\times N}$ and $B_{1\times N}$ are represented in (2.5) and (2.6),

$$A_{1\times N} = \begin{bmatrix} A_1 & A_2 & \dots & A_k & \dots & A_{N-1} & A_N \end{bmatrix} \tag{2.5}$$

$$B_{1\times N} = \begin{bmatrix} B_1 & B_2 & \dots & B_k & \dots & B_{N-1} & B_N \end{bmatrix}. \tag{2.6}$$

The magnitude and phase angle plots of the transfer function, $H(j\omega)$, is found by performing (2.7)-(2.11),

$$FFT\_A_{1\times N} = fft(A_{1\times N}) \tag{2.7}$$

$$FFT\_B_{1\times N} = fft(B_{1\times N}) \tag{2.8}$$

$$H_{k=1}^{N} = \frac{FFT\_B_k}{FFT\_A_k}. \tag{2.9}$$

On performing (2.7)-(2.9), an array of complex numbers is obtained, which is essentially the representation of the transfer function in rectangular coordinates. Array *H* is then converted to polar form by finding the magnitude and phase angles separately,

$$H\_mag_{k=1}^{N} = |H_k| \tag{2.10}$$

$$H\_phase_{k=1}^{N} = \angle H_k. \tag{2.11}$$

When arrays $H\_mag_{1\times N}$ and $H\_phase_{1\times N}$ are plotted against frequency, magnitude and phase angle plots of transfer function, $H(j\omega)$, are obtained.

2.9 Defining the *threshold* Matrix for Cyber Attack Detection

The algorithm developed to detect cyber attacks in a distribution energy management system is briefly given as:

Step 1 – A base case of the distribution system test bed is created. Magnitude and phase angle plots of the transfer functions between different sets of points in the system (for e.g., *c* and *r, c* and *b,* in Figure (2.1)) are found using the method explained in

Section 2.8. These plots are the base case plots, with which plots will be compared at regular intervals, to check for cyber attack or failure in the system.

Step 2 – Acceptable limits of change are set for each block in the system. This will define the changes in the system up to which the system can tolerate, without issuing an alarm. With each of these changes in the blocks, one at a time, the phase angle plots of the transfer functions between the different sets of points are obtained.

Step 3 – For each type of change in system block, phase angle plots are compared with that of base case transfer functions that were created and stored earlier, as in Step 1. The maximum change in phase angle plots are saved in an array. This is done for all types of acceptable changes in the system blocks and a *threshold* matrix is formed.

The transfer functions monitored are,

$TF_{p\to q}$ - Transfer function between *p* and *q*

where *p* is the input and *q* is the output. See Figure (2.1). Note that the $\{p,q\}$ pairs used are $\{c,a\}$, $\{c,r\}, \{c,b\}, \{c,d\}, \{r,b\}$ and $\{e,d\}$.

The base case is taken to be the case when the blocks are all as shown in Figure (2.3) and DLMP input price signal is 0.15 $/kWh. The system, at any point, is compared with this case for any cyber attacks in the distribution energy management system. The calculated transfer functions (e.g., $H_{calc}(j\omega)$) are then examined in the frequency domain to obtain the phase of $H_{calc}(j\omega)$. These phase characteristics are then compared to the base case phase characteristics, $\angle H_{base}(j\omega)$.

If a difference is detected between $\angle H_{calc}(j\omega)$ and $\angle H_{base}(j\omega)$, then one may suspect a cyber attack. The maximum values of,

$$\Delta = \left|\angle H_{calc}(j\omega) - \angle H_{base}(j\omega)\right| \tag{2.12}$$

are shown in Table (2.1) for the indicated six transfer functions. Note that entries in this table are not all zero because changes in the input DLMP impacts Δ. For example, if the base case of 0.15 \$/kWh changes to 0.1 \$/kWh, a phase difference, $\Delta = 2.405$ degree results for $TF_{c\to a}$. Since the input DLMP price signal can vary from 0.01 \$/kWh to a maximum of 0.25 \$/kWh, there should be an alarm only when the price exceeds 0.25 \$/kWh. Hence, the threshold for changes in block *P* is set to take the values corresponding to the phase angle differences when the price is 0.25 \$/kWh.

The frequencies at which the maximum angle differences occur are also noted. The resolution of frequency step in the tests is $\Delta\Omega = \frac{\pi}{100}$ rad/s. A better estimate of frequency at which maximum phase angle difference occurs could be obtained by varying the time step appropriately. The time step denotes the time interval after which the subsequent signal is recorded from the test bed. The time step used in the tests is $\Delta t = 0.01$ second. Parameters in the various transfer functions are changed to calculate threshold values for detection of cyber attacks. Each of the blocks (*Q, Q', R, S, T*) is increased/decreased by 5%, keeping the DC gain of the transfer function constant, and the maximum differences in phase angle values of all transfer functions are noted. For example, the transfer function of block *S*, as shown in (2.13) is modified by +5% to (2.14),

$$H_S(s) = \frac{10}{s+10} \tag{2.13}$$

$$H_S'(s) = \frac{(10)(1.05)}{s + (10)(1.05)} = \frac{10.5}{s + 10.5}. \tag{2.14}$$

Numerator and trailing terms of the denominator are multiplied by 1.05 because the gain of the transfer function has to be constant at steady state. If only one of the terms were changed, the DC gain of the transfer function would be modified. At least in theory, a change in DC gain would be readily detected. In order to identify minor changes in the system, thresholds on phase angle differences are set based on changes that do not change the DC gain of the transfer function. The maximum phase angle differences for the changes denoted are displayed in Table (2.2). The frequencies at which the maximum phase angle differences occur are also specified in the table.

Table (2.1) Phase Angle Differences in Transfer Functions for Changes in DLMP Input

Input DLMP price signal '*P*' ($/kWh)	**Maximum difference in phase angle (in degrees) of indicated transfer functions** **Frequency at which this maximum phase angle difference occurs (rad/s)**					
	$TF_{c\to a}$	$TF_{c\to r}$	$TF_{c\to b}$	$TF_{c\to d}$	$TF_{r\to b}$	$TF_{e\to d}$
0.01	4.9201 at $\omega = 12.5978$	0.0374 at $\omega = 2.0106$	0.0347 at $\omega = 2.0106$	3.1242 at $\omega = 16.1164$	0.0027 at $\omega = 2.0106$	3.1507 at $\omega = 16.0535$
0.05	3.9891 at $\omega = 12.2522$	0.031 at $\omega = 2.0106$	0.0287 at $\omega = 2.0106$	2.5384 at $\omega = 15.8022$	0.0022 at $\omega = 2.0106$	2.5608 at $\omega = 15.708$
0.1	2.405 at $\omega = 11.7181$	0.0194 at $\omega = 2.0106$	0.018 at $\omega = 2.0106$	1.5349 at $\omega = 15.2681$	0.0014 at $\omega = 2.0106$	1.5495 at $\omega = 15.1739$
0.15	0	0	0	0	0	0
0.2	4.1877 at $\omega = 9.8960$	0.0387 at $\omega = 2.0106$	0.0359 at $\omega = 2.0106$	2.6897 at $\omega = 13.3518$	0.0028 at $\omega = 2.0106$	2.7241 at $\omega = 13.2261$
0.25	14.0551 at $\omega = 7.8540$	0.1547 at $\omega = 2.0106$	0.1436 at $\omega = 2.0106$	9.0013 at $\omega = 11.0898$	0.0111 at $\omega = 2.0106$	9.1759 at $\omega = 10.9642$

Table (2.2) Phase Angle Differences in Transfer Functions for Changes in Blocks Q, Q', R, S, T

Type of change in the system		**Maximum difference in phase angle (in degrees) of transfer functions** **Frequency at which this maximum phase angle difference occurs (rad/s)**					
		$TF_{c\to a}$	$TF_{c\to r}$	$TF_{c\to b}$	$TF_{c\to d}$	$TF_{r\to b}$	$TF_{e\to d}$
ΔQ, $\Delta Q'$	**+5%**	0.7091 at $\omega = 10.7128$	0.0295 at $\omega = 2.0106$	0.0223 at $\omega = 2.0106$	0.6046 at $\omega = 14.2000$	0.0079 at $\omega = 2.7960$	0.6104 at $\omega = 14.1372$
	-5%	0.6610 at $\omega = 11.0898$	0.0305 at $\omega = 2.0106$	0.0233 at $\omega = 2.0106$	0.5677 at $\omega = 14.7341$	0.0080 at $\omega = 2.7646$	0.5727 at $\omega = 14.7027$
ΔR	**+5%**	0.0930 at $\omega = 2.0106$	0.0934 at $\omega = 2.0106$	0.0835 at $\omega = 2.0106$	0.0882 at $\omega = 2.0106$	0.0113 at $\omega = 3.2044$	0.0046 at $\omega = 21.9597$
	-5%	0.0929 at $\omega = 2.0106$	0.0933 at $\omega = 2.0106$	0.0834 at $\omega = 2.0106$	0.0880 at $\omega = 2.0106$	0.0113 at $\omega = 2.2044$	0.0045 at $\omega = 21.9597$
ΔS	**+5%**	0.0141 at $\omega = 2.8903$	0.0001 at $\omega = 3.3929$	0.0132 at $\omega = 2.8903$	0.0140 at $\omega = 2.9531$	0.0132 at $\omega = 2.8588$	0.0019 at $\omega = 15.4881$
	-5%	0.0157 at $\omega = 2.8274$	0.0001 at $\omega = 3.3301$	0.0148 at $\omega = 2.8274$	0.0156 at $\omega = 2.8903$	0.0147 at $\omega = 2.7960$	0.0022 at $\omega = 15.3938$
ΔT	**+5%**	2.0643 at $\omega = 3.3929$	0.0299 at $\omega = 2.1049$	0.0309 at $\omega = 2.0106$	1.9481 at $\omega = 3.2987$	0.0061 at $\omega = 4.6181$	1.9295 at $\omega = 3.3615$
	-5%	2.1487 at $\omega = 3.2358$	0.0326 at $\omega = 2.0106$	0.0334 at $\omega = 2.0106$	2.0246 at $\omega = 3.1416$	0.0063 at $\omega = 4.4611$	2.0040 at $\omega = 3.2044$

With reference to Table (2.2), the phase angle difference value lesser in magnitude out of the +5% and -5% changes is chosen as a threshold. This is done to detect a cyber attack. If the cited threshold is set too large, one may incur a *false dismissal.* This is a term applied when a faulty condition is dismissed as normal. On the other hand, setting a lower value of threshold could cause a *false alarm.* A *false alarm* is the term given to an alarm caused by a normally functioning system. The threshold matrix is found to be,

$$threshold = \begin{bmatrix} 14.0551 & 0.1547 & 0.1436 & 9.0013 & 0.0111 & 9.1759 \\ 0.6610 & 0.0295 & 0.0223 & 0.5677 & 0.0079 & 0.5727 \\ 0.0929 & 0.0933 & 0.0834 & 0.0880 & 0.0113 & 0.0045 \\ 0.0141 & 0.0001 & 0.0132 & 0.0140 & 0.0132 & 0.0019 \\ 2.0643 & 0.0299 & 0.0309 & 1.9481 & 0.0061 & 1.9295 \end{bmatrix}. \quad (2.15)$$

The foregoing example is presented as an illustration. For other energy management systems, the data shown in (2.15) may be different, but the selection of thresholds and calculation procedure will be the same. The only constraint is that the energy management system should be linear and time invariant.

2.10 Cyber Attack Detection Using *threshold* Matrix

Once the *threshold* matrix is formed as explained in Section 2.9, cyber attacks in the energy management system can be identified. Signals are obtained from the points (*a*, *b*, *c*, *d*, *e*, *r*) by the central distribution control center on a timely basis. The transfer function magnitude and phase plots are obtained using the methods explained, and the phase angle plots are compared with the phase angle plots of the base case transfer functions. On comparing the transfer function phase angle plot values, the maximum phase angle differences for all the transfer functions are stored in an array, *max_ang_diff*,

$$\max\_ang\_diff_{1\times 6} = \begin{bmatrix} \max\left|\angle H_{calc,c\to a} - \angle H_{base,c\to a}\right| \\ \max\left|\angle H_{calc,c\to r} - \angle H_{base,c\to r}\right| \\ \max\left|\angle H_{calc,c\to b} - \angle H_{base,c\to b}\right| \\ \max\left|\angle H_{calc,c\to d} - \angle H_{base,c\to d}\right| \\ \max\left|\angle H_{case,r\to b} - \angle H_{base,r\to b}\right| \\ \max\left|\angle H_{calc,e\to d} - \angle H_{base,e\to d}\right| \end{bmatrix}^T . \quad (2.16)$$

In (2.16) the maxima shown in the vector on the right hand side represents the maxima over frequency, ω. This array $\max\_ang\_diff_{1\times 6}$ is compared with each row of the *threshold* matrix. If each element of the array $\max\_ang\_diff_{1\times 6}$ is greater than the corresponding column element in at least one row of the *threshold* matrix, an alarm is issued. To make this method easier, a *flag* matrix, $\Im$ is defined. The matrix $\Im$ is of the same dimension as the *threshold* matrix. Matrix $\Im$ is initialized to,

$$\Im = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \quad (2.17)$$

As the $\max\_ang\_diff$ array is compared with each row of *threshold* matrix, $\Im$ is updated. If an element in the $\max\_ang\_diff$ array is greater than the corresponding column element in any of the rows in *threshold* matrix, set the flag element in $\Im$ corresponding to the coordinates in *threshold* matrix, to 1. The process is better explained in the flowchart in Figure (2.6).

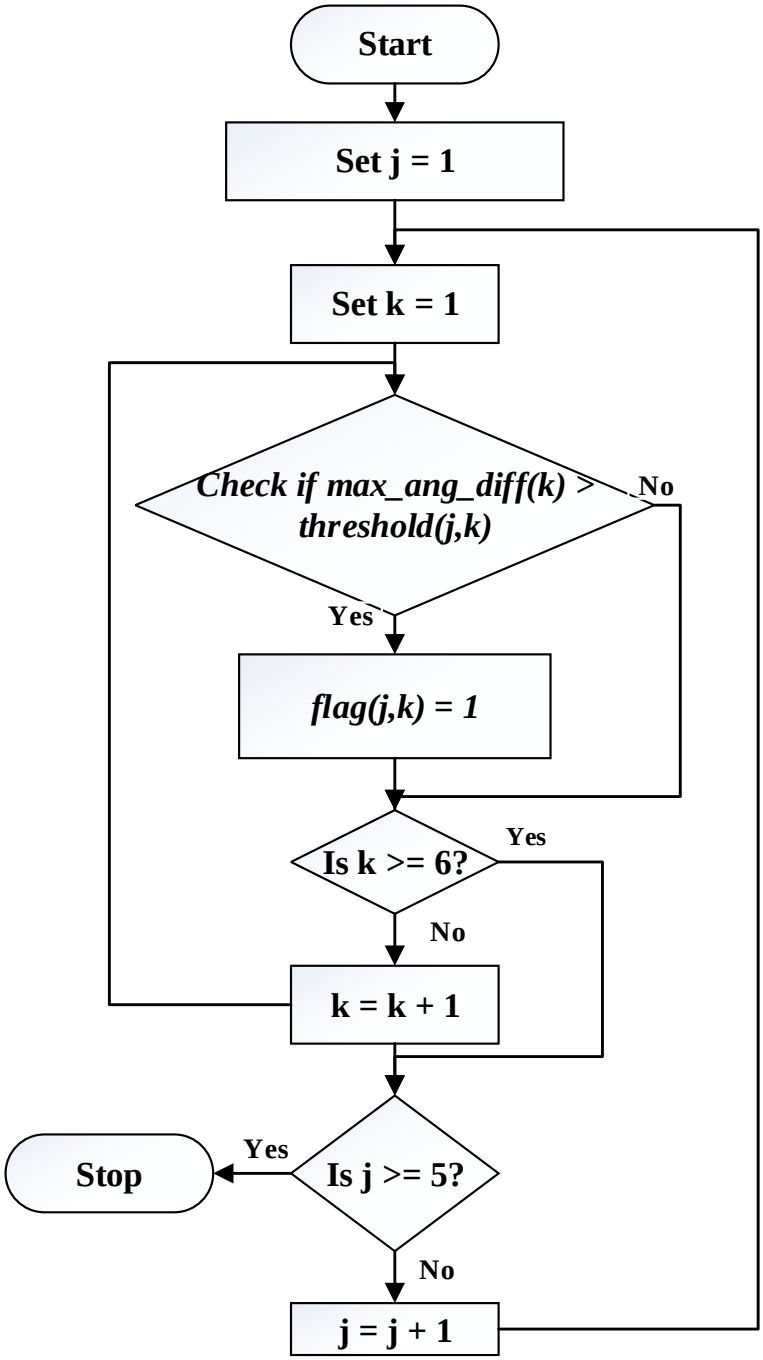

Figure (2.6) Flowchart Explaining *flag* Matrix Modification

Once $\mathfrak{I}$ is updated, sum of each element in a row is calculated for each row of $\mathfrak{I}$. If the row sum is 6, there has been a cyber attack on the system. Mathematically, *row sum* vector, ζ, is calculated as,

$$\zeta = \mathfrak{I} \times \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}. \tag{2.18}$$

If any of the elements of ζ is six, it means there has been a cyber attack on the system. Note that the alarm triggering value in the ζ vector depends on the number of different transfer functions being observed in the system. Since there are six transfer functions being observed in the artifact test bed, the triggering value is six. If there are *n* transfer functions being observed in a system, an alarm is issued if at least one of the elements of ζ turns out to be *n.*

2.11 Summary

To summarize, this chapter explains the following in detail:

- Schematic of the closed loop control system used for tests.
- Components of the test bed (i.e., DLMP input pricing signal, system and sensor dynamics, demand-price relation and price modifying block).
- Algorithm developed to detect cyber attacks in the distribution energy management system by making use of the FFT.
- Defining and obtaining the *threshold* matrix for the test bed.

- Introducing *flag* matrix, $\Im$, and *row sum* matrix, ζ , to check for a cyber attack in the system at regular intervals. In case of a cyber attack, an alarm is issued.

The next chapter will illustrate cyber attack detection using the developed algorithm. This is done with a test bed based on the FREEDM distribution system.

CHAPTER 3

ILLUSTRATIVE APPLICATIONS FOR GENERATING ALARMS: THE NOISE FREE CASE

3.1 Introduction to Test Cases

The preceding chapters explained the schematic of the test bed used to illustrate the algorithm developed to detect cyber attacks in a distribution energy management system. The various blocks in the test bed are all represented as transfer function blocks. Reasons for the selection of the values chosen for the transfer functions have also been explained. Finally, the algorithm developed to detect cyber attacks was explained in detail in Chapter 2. This section will contain illustrations of cyber attacks on the test bed and the validity of the algorithm will be tested.

This chapter deals with an ideal situation i.e., a noise free environment in the system. This means that the numerical signals obtained from different nodes in the system as a function of time are, in fact, the accurate signal values without any error. This might not be a very realistic representation of systems in the real world. To make understanding easier, first the noise free ideal system will be tested with the algorithm in this chapter. Chapter 4 will deal with the noisy case.

3.2 Types of Tests

There are a number of locations in the test bed at which a cyber attack could occur. The list of locations is given in Table (3.1). Since the locations are all transfer function blocks, a cyber attack is illustrated by changing the values of a transfer function block compared to a base case. This way, a number of cyber attacks are illustrated by making different permutation and combination of changes in the blocks. A few examples will be explained and shown in this chapter.

Once a change is depicted in the system, phase plots of the transfer functions between different points in the system are compared with the base case transfer function phase angle plots. As explained in Sections 2.8 – 2.10, the maximum phase angle differences are observed and are compared with the rows of the *threshold* matrix. Finally the *row sum* matrix is created to check for any cyber attacks in the system.

Table (3.1) List of Cyber Attack Locations

Cyber attack location	**Intention of test**	**Nominal (base) value**
P	Test illustrates impact of a cyber attack on the DLMP pricing signal reported at a point of end case.	0.15 $/kWh
Q, Q'	Test illustrates the impact of cyber attack on the elasticity and customer demand response to price.	$\frac{100}{3}$
R	Illustrates the impact of cyber attack on system dynamics.	$\frac{0.04}{s+0.04}$
S	Illustrates the impact of cyber attack on sensor dynamics.	$\frac{10}{s+10}$
T	Illustrates the impact of cyber attack on the price controller block in the system.	$\frac{(30)(0.03)}{s^2+11s+30}$

The following are the cases that are shown in the upcoming sections,

- Case 1 – Change in DLMP pricing signal, represented by *P*, from 0.15 \$/kWh to 0.25 \$/kWh.
- Case 2 – Change in blocks *Q* and *Q'* from $\frac{100}{3}$ to $\frac{95}{3}$.
- Case 3 – Change in block *R* from $\frac{0.04}{s+0.04}$ to $\frac{0.042}{s+0.042}$.
- Case 4 – Change in block *S* from $\frac{10}{s+10}$ to $\frac{10.51}{s+10.51}$.
- Case 5 – Change in block *T* from $\frac{(30)(0.03)}{s^2+11s+30}$ to $\frac{(28.51)(0.03)}{s^2+11s+28.51}$.

All the test cases will use the *threshold* matrix as formed in Section 2.9,

$$threshold = \begin{bmatrix} 14.0551 & 0.1547 & 0.1436 & 9.0013 & 0.0111 & 9.1759 \\ 0.6610 & 0.0295 & 0.0223 & 0.5677 & 0.0079 & 0.5727 \\ 0.0929 & 0.0933 & 0.0834 & 0.0880 & 0.0113 & 0.0045 \\ 0.0141 & 0.0001 & 0.0132 & 0.0140 & 0.0132 & 0.0019 \\ 2.0643 & 0.0299 & 0.0309 & 1.9481 & 0.0061 & 1.9295 \end{bmatrix}. \quad (3.1)$$

3.3 Case 1 – Change in *P* Block

In Case 1, consider a change in *P*: 0.15 \$/kWh to 0.25 \$/kWh. According to the *threshold* values set, this change should not issue an alarm. On making the changes and running the simulation on SimuLink and checking for a cyber attack, the following key observations are made,

$$\max\_ang\_diff = \begin{bmatrix} 14.0551 & 0.1547 & 0.1436 & 9.0013 & 0.0111 & 9.1759 \end{bmatrix} \quad (3.2)$$

$$\Im = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \tag{3.3}$$

$$\zeta = \begin{bmatrix} 0 \\ 6 \\ 5 \\ 5 \\ 6 \end{bmatrix}. \tag{3.4}$$

In (3.2), the maxima are in degrees. These results suggest that there is a cyber attack in the system, where there is not. This is one of the situations where an alarm is issued by the automated energy management system during a normal condition, called a *false alarm.* Upon further inspection the alarm will be ruled of as a normal condition. This is a disadvantage of using the algorithm developed. On trial and error, it was found that the algorithm works fine till a DLMP pricing signal of 0.2286 $/kWh. For any input signal greater than 0.2286 $/kWh, a false alarm is issued.

3.4 Case 2 – Change in Blocks *Q* and *Q'*

In Case 2, consider a change in Q and Q' : $\frac{100}{3}$ to $\frac{95}{3}$. According to the *threshold* values set, this change should not issue an alarm. On making the changes and running the simulation on SimuLink and checking for a cyber attack, the following key observations are made,

$$\max\_ang\_diff = \begin{bmatrix} 0.6610 & 0.0305 & 0.0233 & 0.5677 & 0.0080 & 0.5727 \end{bmatrix} \tag{3.5}$$

$$\mathfrak{I} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{3.6}$$

$$\zeta = \begin{bmatrix} 0 \\ 3 \\ 3 \\ 5 \\ 2 \end{bmatrix}. \tag{3.7}$$

In all cases, the maximum phase angle difference values (e.g., (3.5)) are in degrees. These results suggest that there is no cyber attack in the system, which agrees with the values put in. To further check the validity of the algorithm, another change is made to the block and the matrices are checked, i.e., change in Q and Q': $\frac{100}{3}$ to $\frac{94.9}{3}$. This should issue an alarm as the change is more than 5%. The algorithm gives the following results,

$$\max\_ang\_diff = \begin{bmatrix} 0.6737 & 0.0312 & 0.0238 & 0.5787 & 0.0081 & 0.5838 \end{bmatrix} \tag{3.8}$$

$$\mathfrak{I} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{3.9}$$

$$\zeta = \begin{bmatrix} 0 \\ 6 \\ 3 \\ 5 \\ 2 \end{bmatrix}. \tag{3.10}$$

An alarm is issued as at least one of the values in the matrix *row sum* is 6. This further validates the algorithm's functionality.

3.5 Case 3 – Change in Block *R*

In Case 3, consider a change in R : $\frac{0.04}{s+0.04}$ to $\frac{0.042}{s+0.42}$. This is a 5% change in the block and shouldn't trigger an alarm. The key matrices obtained on running the algorithm are,

$$\max\_ang\_diff = \begin{bmatrix} 0.0930 & 0.0934 & 0.0835 & 0.0882 & 0.0113 & 0.0046 \end{bmatrix} \tag{3.11}$$

$$\Im = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix} \tag{3.12}$$

$$\zeta = \begin{bmatrix} 1 \\ 3 \\ 5 \\ 5 \\ 3 \end{bmatrix}. \tag{3.13}$$

Below a change of +5% in block *R* an alarm is not issued. The terminology used here is that a +5% "change in a block" refers to the simultaneous change in numerator and pole value. A negative change in the block is checked too. It appears that the algorithm does not indicate a cyber attack up to a -5% change in the block. It means that there are no false alarms for changes in *R* in the test bed.

On the other hand, if the change is over 5%, the automated energy management system should issue an alarm. Such a case is simulated and the output of the algorithm is observed, change in R : $\frac{0.04}{s+0.04}$ to $\frac{0.0379}{s+0.379}$. Following results are observed due to the change mentioned above,

$$\max\_ang\_diff = \begin{bmatrix} 0.0975 & 0.0979 & 0.0876 & 0.0924 & 0.0119 & 0.0047 \end{bmatrix} \tag{3.14}$$

$$\Im = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix} \tag{3.15}$$

$$\zeta = \begin{bmatrix} 1 \\ 3 \\ 6 \\ 5 \\ 3 \end{bmatrix}. \tag{3.16}$$

This is an indication that there are no *false dismissals*.

3.6 Case 4 – Change in Block *S*

In Case 4, consider a change in S : $\frac{10}{s+10}$ to $\frac{10.51}{s+10.51}$. This is a change of 5.1% to block *S*. Since the *threshold* values are from changes of 5%, this change should trigger an alarm. Simulation is run after the change is made to the system in SimuLink. The matrices obtained are given below,

$$\max\_ang\_diff = \begin{bmatrix} 0.0143 & 0.0001 & 0.0135 & 0.0142 & 0.0134 & 0.002 \end{bmatrix} \tag{3.17}$$

$$\Im = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{3.18}$$

$$\zeta = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 6 \\ 1 \end{bmatrix}. \tag{3.19}$$

While this proves that there are no cases of *false dismissals*, another case shows that there are situations where *false alarms* are issued. A *false alarm* is issued when there is a reduction in the block in the range of 4.51% to 5%.

3.7 Case 5 – Change in Block *T*

In Case 5, consider a change in T : $\frac{(30)(0.03)}{s^2+11s+30}$ to $\frac{(28.51)(0.03)}{s^2+11s+28.51}$. When the specified change occurs, the automated energy management system operator should see it as a normal condition, since the change is less than 5%. Once again, the terminology used here for "a 5% change in a block" refers to a simultaneous 5% change in numerator and trailing denominator parameter. Thus a "5% change" does not affect the DC gain of the block. In this particular example, the 5% change is manifested as $30 \to 28.50$ in the numerator and $30 \to 28.50$ change in the trailing denominator term. In this particular test, the indicated change is less than 5%, and thus the parameter 28.51 is used (representing a change of 4.966%). The change is simulated in SimuLink and the algorithm responds in the following way,

$$\max\_ang\_diff = \begin{bmatrix} 2.1341 & 0.0324 & 0.0332 & 2.0108 & 0.0063 & 1.9904 \end{bmatrix} \tag{3.20}$$

$$\Im = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \tag{3.21}$$

$$\zeta = \begin{bmatrix} 0 \\ 5 \\ 3 \\ 5 \\ 6 \end{bmatrix}. \tag{3.22}$$

This is a case of *false alarm.* On further inspection, the system is found to be functioning in normal condition. By simulating other changes, it is found that there are no cases of *false dismissals* encountered for changes in block *T*.

3.8 Summary of Cases of False Dismissals and False Alarms

From the tests conducted, it can be concluded that there are a few cases of *false alarms*, although there are no *false dismissals*. This is a conservative design – i.e., no false dismissals, but there may be false alarms. The algorithm performance detecting cyber attack in the test bed is summarized in Table (3.2).

Chapter 4 will address the case where noise is present in the system. The types of noise encountered in a distribution energy management system will be addressed and the algorithm will be tested in a noisy test bed.

Table (3.2) Performance of Algorithm for Cyber Attacks in Various Locations in a Noise-free Case

Case number	**Type of change in system**	**False alarm**	**False dismissal**
Case 1	Change in P (base case 0.15 \$/kWh)	$0.2286 < P \leq 0.25$	None
Case 2	Change in Q and Q': $\frac{100(1+\Delta Q)}{3}$ Base case $\Delta Q = 0$	None	None
Case 3	Change in R: $\frac{0.04(1+\Delta R)}{s+0.04(1+\Delta R)}$ Base case $\Delta R = 0$	None	None
Case 4	Change in S: $\frac{10(1+\Delta S)}{s+10(1+\Delta S)}$ Base case $\Delta S = 0$	$-4.5\% > \Delta S \geq -5\%$	None
Case 5	Change in T: $\frac{(30)(0.03)(1+\Delta T)}{s^2+11s+30(1+\Delta T)}$ Base case $\Delta T = 0$	$-4.83\% > \Delta T \geq -5\%$	None

CHAPTER 4

ILLUSTRATIVE APPLICATIONS FOR GENERATING ALARMS: THE NOISY CASE

4.1 Introduction to Noisy Test Cases

This chapter contains illustrations of cyber attacks on the test bed where the input DLMP signal varies with time. The DLMP signal is contaminated with noise for these tests. In the test cases conducted in SimuLink, noise in the DLMP signal is represented by a *random number* block. The *random number* parameters are set depending on the magnitude of signal variation. A signal to noise ratio of 50 is used in the tests conducted. The addition of noise is as shown,

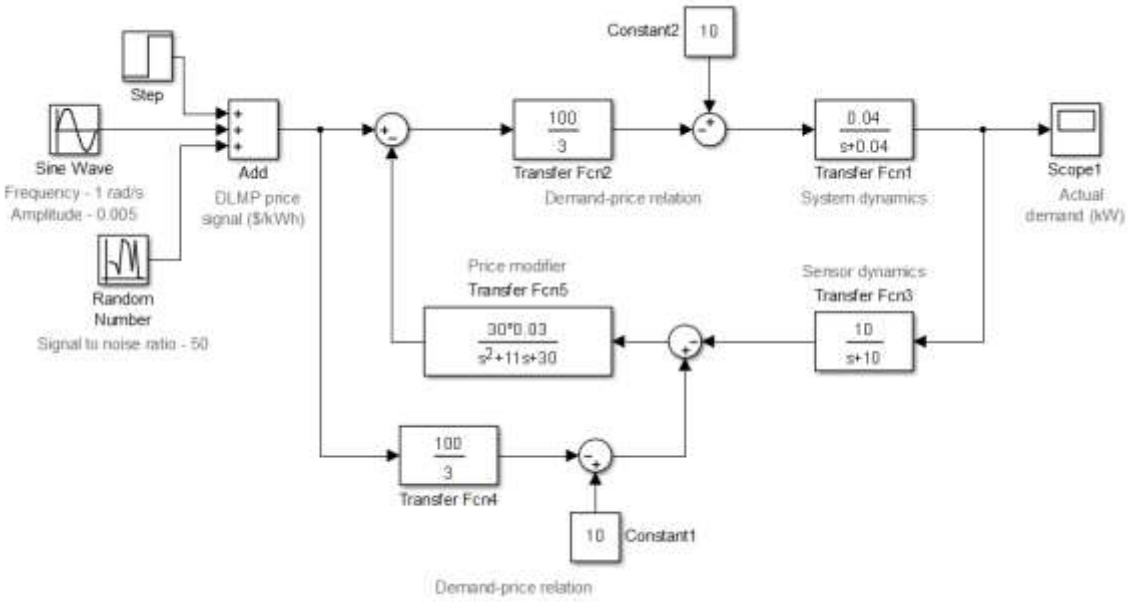

Figure (4.1) Energy Management Control System Test Bed in Noisy Test Cases

On making changes to the input signal to the system, all signal values change and, hence, the important *threshold* matrix is modified too. The new threshold matrix for the noisy case is derived in Section 4.2.

4.2 *Threshold* Matrix for Noisy Cases

As mentioned in earlier sections, the *threshold* matrix changes when there is any change at the input end. The procedure followed to obtain the *threshold* matrix is same as explained in Section 2.9. Although, it is observed that the phase angle of the transfer function between any two points in the system varies anywhere between -180 and 180 degrees at different frequencies. For this reason, the phase angle differences in all the transfer functions above 20 degrees are ignored. They are assumed to be caused by the noise signal at the input. Following the steps explained in detail in Section 2.9, the *threshold* matrix for the noisy case is found as,

$$threshold = \begin{bmatrix} 19.8592 & 0.2593 & 0.2362 & 19.8268 & 0.0850 & 19.9869 \\ 15.048 & 0.0333 & 0.0257 & 1.6484 & 0.0106 & 2.3002 \\ 0.0967 & 0.0906 & 0.0811 & 0.0880 & 0.0122 & 0.0072 \\ 0.1473 & 0.0001 & 0.0143 & 0.0140 & 0.0142 & 0.0040 \\ 13.8161 & 0.0305 & 0.0313 & 1.9534 & 0.0064 & 1.9362 \end{bmatrix}. \quad (4.1)$$

4.3 Type of Tests

Since the test bed created is the same as in the noise free case, the locations where a cyber attack could occur are the same as in Chapter 3. The list of cyber attack locations is given in Table (4.1).

The following are the cases that are shown in the upcoming sections,

- Case 1 – Change in DLMP pricing signal, represented by *P*, from 0.15 $/kWh to 0.25 $/kWh.
- Case 2 – Change in blocks *Q* and *Q'* from $\frac{100}{3}$ to $\frac{95}{3}$.

- Case 3 – Change in block *R* from $\frac{0.04}{s+0.04}$ to $\frac{0.042}{s+0.042}$.
- Case 4 – Change in block *S* from $\frac{10}{s+10}$ to $\frac{10.51}{s+10.51}$.
- Case 5 – Change in block *T* from $\frac{(30)(0.03)}{s^2+11s+30}$ to $\frac{(28.51)(0.03)}{s^2+11s+28.51}$.

Table (4.1) List of Cyber Attack Locations

Cyber attack location	**Intention of test**	**Nominal (base) value**
P	Test illustrates impact of a cyber attack on the DLMP pricing signal reported at a point of end case.	0.15 $/kWh
Q, Q'	Test illustrates the impact of cyber attack on the elasticity and customer demand response to price.	$\frac{100}{3}$
R	Illustrates the impact of cyber attack on system dynamics.	$\frac{0.04}{s+0.04}$
S	Illustrates the impact of cyber attack on sensor dynamics.	$\frac{10}{s+10}$
T	Illustrates the impact of cyber attack on the price controller block in the system.	$\frac{(30)(0.03)}{s^2+11s+30}$

A "base case" is simulated and the phase angle values are stored for all the transfer functions. The test case will be simulated and the phase angle plots of the transfer functions will be compared with that of the base case. In the upcoming sections, different cyber attacks are simulated and the following are displayed for each case:

- An array, *max_ang_diff*, containing the maximum phase angle differences, in degrees, observed in each transfer function phase characteristics.
- *Flag* matrix, $\Im$, depicting the locations of violations in the *threshold* matrix.
- Vector *row sum*, ζ, indicating if a cyber attack has been detected or not.

Also, "an *n%* change in a block" refers to a simultaneous *n%* change in numerator and trailing denominator parameter.

4.4 Case 1 – Change in *P* Block

In Case 1, consider a change in *P*: 0.15 $/kWh to 0.25 $/kWh. According to the *threshold* values set, this change should not issue an alarm. On making the changes and running the simulation on SimuLink and checking for a cyber attack, the following key observations are made,

$$\max\_ang\_diff = \begin{bmatrix} 19.8592 & 0.2593 & 0.2362 & 19.8268 & 0.0850 & 19.9869 \end{bmatrix} \tag{4.2}$$

$$flag = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \tag{4.3}$$

$$\zeta = \begin{bmatrix} 0 \\ 6 \\ 6 \\ 6 \\ 6 \end{bmatrix}. \tag{4.4}$$

The *row sum* matrix indicates the existence of a cyber attack, when there is none. This is a case of false alarm. On simulation of more cases, it is observed that a relatively small change in the input DLMP signal causes a false alarm. Any pricing signal above 0.1806 $/kWh causes a false alarm. This is solely due to the presence of a noise component as this is not the case with that of the noise free tests.

4.5 Case 2 – Change in Blocks *Q* and *Q'*

In Case 2, consider a change in Q and Q' : $\frac{100}{3}$ to $\frac{95}{3}$. According to the *threshold* values set, this change should not issue an alarm. On making the changes and running the simulation on SimuLink and checking for a cyber attack, the following key observations are made,

$$\max\_ang\_diff = \begin{bmatrix} 19.1167 & 0.0336 & 0.0259 & 1.6484 & 0.0106 & 2.3002 \end{bmatrix} \tag{4.5}$$

$$\Im = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix} \tag{4.6}$$

$$\zeta = \begin{bmatrix} 0 \\ 3 \\ 3 \\ 5 \\ 4 \end{bmatrix}. \tag{4.7}$$

The algorithm does not produce any *false dismissal*. Similarly, there are no *false alarms* too. To indicate that a cyber attack is detected when there is a change of over 5%, consider changes in blocks Q and Q': $\frac{100}{3}$ to $\frac{94.9}{3}$. The following observations are made,

$$\max\_ang\_diff = \begin{bmatrix} 19.5227 & 0.0343 & 0.0264 & 1.6807 & 0.0108 & 2.3416 \end{bmatrix} \tag{4.8}$$

$$\Im = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix} \tag{4.9}$$

$$\zeta = \begin{bmatrix} 0 \\ 6 \\ 3 \\ 5 \\ 4 \end{bmatrix}. \tag{4.10}$$

The *row sum* vector, ζ, indicates that there is a cyber attack in the system. This indicates that a cyber attack on Q and Q' is never dismissed as a normal condition.

4.6 Case 3 – Change in *R* Block

In Case 3, consider a change in R: $\frac{0.04}{s+0.04}$ to $\frac{0.042}{s+0.42}$. This is a +5% change in the block and should not trigger an alarm. The matrices obtained on running the algorithm are,

$$\max\_ang\_diff = \begin{bmatrix} 0.0968 & 0.0908 & 0.0812 & 0.0882 & 0.0122 & 0.0075 \end{bmatrix} \tag{4.11}$$

$$\Im = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix} \tag{4.12}$$

$$\zeta = \begin{bmatrix} 0 \\ 3 \\ 5 \\ 4 \\ 3 \end{bmatrix}. \tag{4.13}$$

Below a change of +5% in block *R*, an alarm is not issued. A negative change in the block is checked too. It appears that the algorithm does not indicate a cyber attack up to a -5% change in the block. It means that there are no false alarms for changes in *R* in the test bed.

On the other hand, if the change is over 5%, the automated energy management system should issue an alarm. Such a case is simulated and the output of the algorithm is observed, change in R : $\frac{0.04}{s+0.04}$ to $\frac{0.0379}{s+0.379}$. The algorithm produces the following results,

$$\max\_ang\_diff = \begin{bmatrix} 0.1015 & 0.0952 & 0.0851 & 0.0924 & 0.0128 & 0.0075 \end{bmatrix} \tag{4.14}$$

$$\Im = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix} \tag{4.15}$$

$$\zeta = \begin{bmatrix} 0 \\ 3 \\ 6 \\ 4 \\ 3 \end{bmatrix}. \tag{4.16}$$

This is an indication that there are no *false dismissals*.

4.7 Case 4 – Change in *S* Block

In Case 4, consider a change in S : $\frac{10}{s+10}$ to $\frac{10.51}{s+10.51}$. This is a change of 5.1% to block *S*. Since the *threshold* values are from changes of 5%, this change should trigger an alarm. Simulation is run after the change is made to the system in SimuLink.

$$\max\_ang\_diff = \begin{bmatrix} 0.1501 & 0.0001 & 0.0146 & 0.0142 & 0.0145 & 0.0041 \end{bmatrix} \tag{4.17}$$

$$\Im = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{4.18}$$

$$\zeta = \begin{bmatrix} 0 \\ 1 \\ 2 \\ 6 \\ 1 \end{bmatrix}. \tag{4.19}$$

This is an indication that a cyber attack is detected by the algorithm. On running more tests, it could be observed that there are no *false dismissals*. Similarly, if a block change of -5% was simulated, the following is observed,

$$\max\_ang\_diff = \begin{bmatrix} 0.1591 & 0.0001 & 0.0160 & 0.0156 & 0.0159 & 0.0044 \end{bmatrix} \tag{4.20}$$

$$\Im = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{4.21}$$

$$\zeta = \begin{bmatrix} 0 \\ 1 \\ 2 \\ 6 \\ 1 \end{bmatrix}. \tag{4.22}$$

The *row sum* vector indicates a cyber attack when there is not one. This is a *false alarm*. On running more tests it could be concluded that a *false alarm* is issued for changes in the range $-4.64\% > \Delta S \geq -5\%$. There are no *false dismissals.*

4.8 Case 5 – Change in Block *T*

In Case 5, consider a change in T : $\frac{(30)(0.03)}{s^2+11s+30}$ to $\frac{(28.51)(0.03)}{s^2+11s+28.51}$. When the specified change occurs, the automated energy management system operator should see it as a normal condition, since the change is less than 5%. In this particular example, the 5% change is manifested as $30 \rightarrow 28.50$ in the numerator and $30 \rightarrow 28.50$ change in the trailing denominator term. In this particular test, the indicated change is less than 5%, and thus the parameter 28.51 is used (representing a change of 4.966%). The change is simulated in SimuLink and the algorithm responds in the following way,

$$\max\_ang\_diff = \begin{bmatrix} 18.4388 & 0.0330 & 0.0334 & 2.0128 & 0.0067 & 1.9922 \end{bmatrix} \tag{4.23}$$

$$\mathfrak{I} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \tag{4.24}$$

$$\zeta = \begin{bmatrix} 0 \\ 3 \\ 3 \\ 5 \\ 6 \end{bmatrix}. \tag{4.25}$$

This is another case of *false alarm* issued. On running more cases it is observed that there are no *false dismissals* and *false alarms* issued for changes in the range $-4.8\% > \Delta T \geq -5\%$.

4.9 Summary of Cases of *false alarms* and *false dismissals*

From the tests conducted, it can be concluded that there are a few cases of *false alarms*, although there are no *false dismissals*. Changes in block *P*, in particular, produce too many false alarms. Although this is not a good thing, the DLMP price signal is the signal that could be accessed the easiest. This means that a *false alarm* produced due to an acceptable change in the input DLMP signal could be detected easily on inspection and the system could be taken off a state of cyber attack. This is a conservative design – i.e., no *false dismissals*, but there may be *false alarms*. The algorithm performance detecting cyber attack in the test bed is summarized in Table (4.2).

Table (4.2) Performance of Algorithm for Cyber Attacks in Various Locations in a Noisy Case

Case number	**Type of change in system**	**False alarm**	**False dismissal**
Case 1	Change in P (base case 0.15 \$/kWh)	$0.1806 < P \le 0.25$	None
Case 2	Change in Q and Q' : $\frac{100(1+\Delta Q)}{3}$ Base case $\Delta Q = 0$	None	None
Case 3	Change in R: $\frac{0.04(1+\Delta R)}{s+0.04(1+\Delta R)}$ Base case $\Delta R = 0$	None	None
Case 4	Change in S : $\frac{10(1+\Delta S)}{s+10(1+\Delta S)}$ Base case $\Delta S = 0$	$-4.64\% > \Delta S \ge -5\%$	None
Case 5	Change in T : $\frac{(30)(0.03)(1+\Delta T)}{s^2+11s+30(1+\Delta T)}$ Base case $\Delta T = 0$	$-4.8\% > \Delta T \ge -5\%$	None

4.10 Comparison with an Existing Method of Cyber Attack Detection

One of the algorithms developed proposes using an online data validation framework, which verifies that the measurements from the home energy meters match with the measurements obtained from various verification points in the system (feeder level, subsystem level, customer

level) [26]. Though this method was proved to work fine in most of the cases, a few types of cybertampering could be missed by the online validation method.

The method adopted in [26] is explained briefly. The check for cyber attack is done at different levels in a feeder-to-user manner. First, the availability and integrity of the FRTUs is checked at the feeder level. This is achieved by analyzing the log information recorded by the FRTUs. An FRTU is deemed unreliable if malfunction events are observed from its log information. The next step of validation is done at the subsystem level. Power flow is performed and a *mismatch ratio,* which indicates the level of inconsistency of metering data, is defined for each subsystem. The subsystems that have a *mismatch ratio* higher than a set threshold level are determined to be affected by cyber attacks. Once the faulty subsystem(s) is(are) identified, a pattern recognition method is adopted to detect the customers that have been sending out faulty data.

The advantages of the algorithm developed in this thesis over the method adopted in [26] are explained in detail:

- In [26], while performing the power flow analysis at the subsystem level, a cyber attack is detected only when the mismatch ratio exceeds a particular value. This means that a cyber attack is issued when the overall power consumed by the customers in the subsystem (obtained from the home energy meters) differs from the power consumption measured at the subsystem FRTU. This type of a detection leaves out cases where the consumption of various customers are tampered with, keeping the overall consumption same.

  For example, assume a case where there are two customers *A* and *B* in the same subsystem. If customer *A* tampers with the energy meter reading and reduces it by

an amount Δ, and in turn increases the energy meter reading of B by Δ, a cyber attack is not detected. This is a case of what has already been defined as *false dismissal.*

- In [26], there could be possibilities of errors between actual power losses and estimated losses while calculating the *mismatch ratio* for the subsystems. This is because of the difference in the sampling frequency of data for the FRTU and home energy meters. If the estimated power losses are far off from the actual values, it could lead to incorrect *mismatch ratio* and potentially a *false dismissal*.

The advantage with the algorithm developed in this thesis is that there are no *false dismissals*. A cyber attack is always detected.

Though there are a few advantages of using the algorithm implemented in this work over the method adopted in [26], there is a disadvantage of using the same too. The disadvantage is that signals have to be obtained from various sections in a system. This requires many sensors and data communication devices. Another disadvantage is the need for large memory storage devices storing the data collected from the sensors at regular intervals of time.

CHAPTER 5

CONCLUSIONS AND FUTURE WORK

5.1 Conclusions

The aim of this thesis is to develop an algorithm to detect cyber attacks in a distribution energy management system. Each component and element in a single customer distribution system is designed and built using transfer function blocks, in the *s*-domain. Four main elements of the energy management system are represented by linear transfer functions. If other transfer functions are used in an actual energy management system, it is believed that those transfer functions could be substituted. The data used in the transfer functions are taken as representative of the energy management used in the FREEDM system. The entire concept is based on the architecture of the FREEDM system.

Signals from various points in the system are taken to obtain the frequency response of the transfer functions between the respective sets of points in the system. A base case is simulated and the phase angles are stored. The objective is to detect a cyber attack by studying the phase angle curves of the transfer functions at regular intervals. A threshold is set on the permissible amount of change in phase angle values of each transfer function compared to the base case values. This threshold is set by obtaining the maximum phase angle differences seen on simulating 5% changes in various blocks in the system. If the differences are higher than the set threshold, a cyber attack is said to be detected and an alarm is issued. This algorithm is explained in detail in Chapter 2. The algorithm is tested on a noise free test bed in Chapter 3 and a noisy test bed in Chapter 4.

Note that a change in excess of 5% in any of the blocks should be considered as "detectable cyber attacks" and any change below that should be considered normal. The value "5%" is an arbitrary value. A reasonably conservative limit is set on the permissible change in the blocks. Otherwise, the constantly varying nature of the input DLMP pricing signal could cause numerous cases of *false alarms*.

It can be concluded from the results of the tests conducted to test the algorithm in a noise free case that the algorithm is efficient and there are very few cases of *false alarms* and no *false dismissals*. The important observations from the tests conducted are described in Table 5.1.

Table (5.1) Results of Noise-free Test Cases

Case number	**Type of change in system**	**False alarm**	**False dismissal**
Case 1	Change in P (base case 0.15 \$/kWh)	$0.2286 < P \leq 0.25$	None
Case 2	Change in Q and Q': $\frac{100(1+\Delta Q)}{3}$ Base case $\Delta Q = 0$	None	None
Case 3	Change in R: $\frac{0.04(1+\Delta R)}{s+0.04(1+\Delta R)}$ Base case $\Delta R = 0$	None	None
Case 4	Change in S: $\frac{10(1+\Delta S)}{s+10(1+\Delta S)}$ Base case $\Delta S = 0$	$-4.5\% > \Delta S \geq -5\%$	None
Case 5	Change in T: $\frac{(30)(0.03)(1+\Delta T)}{s^2+11s+30(1+\Delta T)}$ Base case $\Delta T = 0$	$-4.83\% > \Delta T \geq -5\%$	None

Similar tests are conducted for the noisy case, where the input pricing signal has a noise component. The noise component is represented by a random number generation block. This is a closer representation of the real time DLMP signal. The output of the tests are similar to that of the noise free cases. There are no cases of *false dismissals*, although there are cases of *false alarms*. It could be noted that the number of false alarms is high due to changes in the DLMP price input. The important features are concluded in Table 5.2.

Table (5.2) Results of Noisy Test Cases

Case number	**Type of change in system**	**False alarm**	**False dismissal**
Case 1	Change in P (base case 0.15 \$/kWh)	$0.1806 < P \leq 0.25$	None
Case 2	Change in Q and Q': $\frac{100(1+\Delta Q)}{3}$ Base case $\Delta Q = 0$	None	None
Case 3	Change in R: $\frac{0.04(1+\Delta R)}{s+0.04(1+\Delta R)}$ Base case $\Delta R = 0$	None	None
Case 4	Change in S: $\frac{10(1+\Delta S)}{s+10(1+\Delta S)}$ Base case $\Delta S = 0$	$-4.64\% > \Delta S \geq -5\%$	None
Case 5	Change in T: $\frac{(30)(0.03)(1+\Delta T)}{s^2+11s+30(1+\Delta T)}$ Base case $\Delta T = 0$	$-4.8\% > \Delta T \geq -5\%$	None

A main conclusion of this work is that detection of changes in phase angle of digitally (on-line) calculated transfer functions of components of an energy management system is a valid method to detect cyber attacks.

5.2 Recommendations for Future Work

Future work remains for improvement and analysis of the developed cyber attack detection algorithm, including:

- implementation on different test beds, perhaps actual commercially implemented energy management systems
- use a real time DLMP signal as the input pricing signal (e.g., obtained from contemporary data in place at one of the Independent System Operators in the United States)
- an improvement of the approximation of customer price-demand relation by studying load profiles
- development of a method to reduce the number of *false alarms.*

REFERENCES

[1] Alex Huang, "FREEDM system – A vision for the future grid," *Power and Energy Society General Meeting*, IEEE, Minneapolis, Minnesota, USA, 2010.

[2] FREEDM Systems Center, "FREEDM Education," 2014, http://www.freedm.ncsu.edu/index.php?s=5

[3] M. Baran, A. Q. Huang and G. G. Karady, "FREEDM system: An electronic Smart Distribution Grid for the future," *Transmission and Distribution Conference and Exposition*, IEE PES, Orlando, Florida, USA, 2012.

[4] FREEDM Systems Center, "About: FREEDM Systems," 2014, http://www.freedm.ncsu.edu/index.php?s=1&p=6

[5] M. Baran, S. Bhattacharya, A. Q. Huang, S. Lukic and X. She, "Performance evaluation of solid state transformer based microgrid in FREEDM systems," *Applied Power Electronics Conference and Exposition (APEC)*, Fort Worth, Texas, USA, 2011.

[6] Y. Jiang, H. Li and P. Tatcho, "A novel line section protection for the FREEDM system based on the solid state transformer," *Power and Energy Society General Meeting*, San Diego, California, USA, 2011.

[7] Gerald T. Heydt, "Future renewable electrical energy delivery and management systems: Energy reliability assessment of FREEDM systems," *Power and Energy Society General Meeting*, Minneapolis, Minnesota, USA, 2010.

[8] S. Bhattacharyya, M. L. Crow, B. McMillin and W. Wang, "Intelligent energy management of the FREEDM system," *Power and Energy Society General Meeting*, Minneapolis, Minnesota, USA, 2010.

[9] Mesut Baran and Mischa Steurer, "A digital testbed for FREEDM system development," *Power and Energy Society General Meeting*, Minneapolis, Minnesota, USA, 2010.

[10] H. Li, L. Liu, P. Tatcho and Y. Zhou, "A real time digital test bed for a Smart Grid using RTDS," *II IEEE International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, Hefei, China, 2010.

[11] Chi-Tsong Chen, *Linear system theory and design*, III edition, Oxford University Press, New York, USA, 1999.

[12] Shlomo Engelberg, *Digital signal processing: An experimental approach*, 2008 edition, Springer-Verlag London Limited, London, United Kingdom, 2008.

[13] Benjamin C. Kuo, *Automatic control systems,* III Edition, Prentice-Hall, Inc., 1975.
[14] N. C. Jagan, *Control systems,* II Edition, B. S. Publications, Hyderabad, India, 2008.

[15] W. Bolton, *Control systems,* I Edition, Elsevier Ltd., Oxford, 2002.

[16] A. A. Rodriguez, *Analysis and design of feedback control systems*, III edition, Tempe, Arizona, 2003.

[17] M. A. Bernstein and J. Griffin, "Regional differences in the price-elasticity of demand for energy," *Infrastructure, Safety, and Environment*, Natural Renewable Energy Laboratory, 2005.

[18] A. Faruqui, S. Sergici and A. Sharif, "The impact of informational feedback on energy consumption – A survey of the experimental evidence," *Social Sciences Research Network Working Paper,* May 1, 2009.

[19] J. Kim and P. R. Thimmapuram, "Consumers' price elasticity of demand modeling with economic effects on electricity markets using an agent-based model," *IEEE Transactions on Smart Grid*, pp. 390 – 397, Vol. 4, No. 1, March, 2013.

[20] A. Motamedi, W. D. Rosehart and H. Zareipour, "Electricity price and demand forecasting in Smart Grids," *IEEE Transactions on Smart Grid,* pp. 664 – 674, Vol. 3, No. 2, 2012.

[21] P. Cumperayot, D. S. Kirschen, D. de Paiva Mendes and G. Strbac, "Factoring the elasticity of demand in electricity prices," *IEEE Transactions on Power Systems,* pp. 612 – 617, Vol. 15, No.2, May, 2000.

[22] H. M. James, N. B. Nichols and R. S. Phillips, *Theory of servomechanisms*, MIT Radiation Laboratory Series, Vol. 25, McGraw-Hill Book Company, Inc., New York, USA, 1947.

[23] J. E. Gibson, *Non-linear Automatic Control*, McGraw-Hill Book Company, New York, USA, 1963.

[24] L. A. Gould, J. F. Kaiser and G. C. Newton, *Analytical design of linear feedback controls,* John Wiley and Sons, Inc., New York, USA, 1957.

[25] S. B. M. Noor, A. R. Shahemabadi and F. S. Taip, "Analytical formulation of the integral square error for linear stable feedback control system," *2013 IEEE International Conference on Control System, Computing and Engineering*, Penang, Malaysia, November 29 – December 1, 2013.

[26] Y. Guo, P. Jirutitijaroen and Chee-Wooi Ten, "Online data validation for distribution operations against cybertampering," *IEEE Transactions on Power Systems*, pp. 550 – 560, Vol. 29, No. 2, March, 2014.

[27] T. B. Smith, "Electricity theft: a comparative analysis," *Energy Policy*, Elsevier, Dubai, United Arab Emirates, 2003.

[28] M. Baran and T. E. McDermott, "Distribution system state estimation using AMI data," *Power Systems Conference and Exposition (PSCE)*, Seattle, Washington, USA, March 15 – 18, 2009.

[29] N. N. Schulz and H. Wang, "A revised branch current-based distribution system state estimation algorithm and meter placement impact," *IEEE Transactions on Power Systems*, pp. 207 – 213, Vol. 19, No. 1, February, 2004.

[30] Z. J. Simendic, V. C. Strezoski and G. S. Svenda, "In-field verification of the real-time distribution state estimation," *18th International Conference on Electricity Distribution*, Turin, Italy, June, 2005.

[31] B. Renz, "Anticipates and responds to disturbances (self heals)," *Research on the characteristics of a Smart Grid*, NETL Modern Grid Strategy team, U.S Department of Energy, National Energy Technology Laboratory, September 2, 2010.

[32] Anonymous, "A systems view of the modern grid," Office of Electricity Delivery and Energy Reliability, U.S Department of Energy, National Energy Technology Laboratory, January, 2007.

[33] B. S. Vohen, T. L. Davis, T. M. Overman and R. W. Sackman, "High-assurance Smart Grid: A three-part model for Smart Grid control systems," *Proceedings of the IEEE*, pp. 1046 – 1062, Vol. 99, No. 6, June, 2011.

[34] George Gross and Tina Orfanogianni, "A general formulation for LMP evaluation," *Power and Energy Society General Meeting*, San Diego, California, USA, July, 2012.

[35] Fernando L. Alvarado, "Is system control entirely by price feasible?," *Proceedings of the 36th Annual Hawaii International Conference*, System Sciences, Hawaii, USA, January, 2003.

[36] California Independent System Operator, "Locational marginal pricing (LMP): Basics of nodal price calculation,"
http://www.caiso.com/docs/2004/02/13/200402131607358643.pdf

[37] G. H. Cheng, H. He and Z. Xu, "Impacts of transmission congestion on market power in electricity market," *Power System Conference and Exposition,* IEEE PES, pp. 190 – 195, Vol. 1, New York City, USA, October, 2004.

[38] Hossein Daneshi and Zuyi Li, "Some observations on market clearing price and locational marginal price," *IEEE Power Engineering Society General Meeting,* pp. 2042 – 2049, Vol. 2, San Francisco, California, USA, June, 2005.

[39] Behnam Tamimi and Sadegh Vaez-Zadeh, "An optimal pricing scheme in electricity markets considering voltage security cost," *IEEE Transactions on Power Systems,* pp. 451 – 459, Vol. 23, No. 2, May, 2008.

[40] R. E. Bohn, M. C. Caramanis and F. C. Schweppe, "Optimal spot pricing: Practice and theory," *IEEE Transactions on Power Apparatus and Systems,* pp. 3234 – 3245, Vol. PAS-101, No. 9, September, 1982.

[41] B. H. Chowdhury, M. L. Crow, D. Haughton, G. T. Heydt, B. D. Kiefer, F. Meng and B. R. Sathyanarayana, "Pricing and control in the next generation power distribution system," *IEEE Transactions on Smart Grid,* pp. 907 – 914, Vol. 3, No. 2, June, 2012.

[42] Badrul H. Chowdhury and Fanjun Meng, "Distribution LMP-based economic operation for future Smart Grid," *Power and Energy Conference,* Champaign, Illinois, USA, February, 2011.

[43] Severin Borenstein and Stephen Holland, "On the efficiency of competitive electricity markets wit time-invariant retail prices," *RAND Journal of Economics,* pp. 469 – 493, Vol. 36, No. 3, pages 469-493, Autumn, 2005.

[44] Gerald T. Heydt and Nicholas Steffan, "Quadratic programming and related techniques for the calculation of locational marginal prices in distribution systems," *North American Power Symposium,* Champaign, Illinois, USA, September 9 – 11, 2012.

[45] P. Nirbhavane, F. Sahriatzadeh and A. K. Srivastava, "Locational marginal price for distribution system considering demand response," *North American Power Symposium*, Champaign, Illinois, USA, September 9 – 11, 2012.

[46] J. Britton, L. Coffeen and J. Rickmann, "A new technique to detect winding displacements in power transformers using frequency response analysis," *Powertech Conference Proceedings,* Bologna, Italy, June 23 – 26, 2003.

[47] C. Ekanayake, T. K. Saha and M. F. M. Yousof, "Study of transformer winding deformation by frequency response analysis," *IEEE Power and Energy Society General Meeting,* Vancouver, British Columbia, Canada, July 21 – 25, 2013.

[48] S. S. Gui, Z. J. Jin, F. H. Wang and J. Xu, "Experimental research of vibration sweep frequency response analysis to detect the winding deformation of power transformer," *Transmission and Distribution Conference and Exposition,* IEEE PES, New Orleans, Los Angeles, April 19 – 22, 2010.

[49] A. Abu-Siada, N. Hashemnia, S. Islam and M. A. S. Masoum, "Understanding power transformer frequency response analysis signatures," *IEEE Electrical Insulation Magazine*, pp. 48 – 56, Vol. 29, Issue 3, April 25, 2013.

APPENDIX

MATLAB CODE USED FOR ANALYSIS OF THE TEST BED

A.1 INITIAL BASE CASE CALCULATION

```
%%%%%%%%%%%%%%%%%%%%%%%%%     BASE_CASE
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Time of which the simulation is run in SimuLink
n = 200;
% Time step used
T = 0.01;
% Finding the sampling frequency
Fs = 1/T;
% Finding the total number of signal values
L = n*Fs;
% Finding the mid point so that the second half of the fourier
transfer can
% be ignored
h = L/2+1;
% Generating the frequency array corresponding to which the
phase angles will
% have to be plotted
f = Fs/2*linspace(0,1,h);
% Converting the frequency from Hertz to radian per second
f = f*2*pi;
% Finding the phase plots of the transfer functions between dif-
ferent sets of
% points in the test bed
[initial_ang1] = phase_angle_calc (c,a);
[initial_ang2] = phase_angle_calc (c,r);
[initial_ang3] = phase_angle_calc (c,b);
[initial_ang4] = phase_angle_calc (c,d);
[initial_ang5] = phase_angle_calc (r,b);
[initial_ang6] = phase_angle_calc (e,d);


%%%%%%%%%%%%%%%%%%%%%%%%%     PHASE_ANGLE_CALC
%%%%%%%%%%%%%%%%%%%%%%%%
% Function used to obtain the phase angle plots of the base case
of the
% system
% ang - phase angle plot between 'input' and 'output'
% input - input signal array
% output - output signal array
function [ang] = phase_angle_calc (input,output)
% Setting the ending frequency of 20 rad/s
final = 650;
% Finding the Fast Fourier Transform of the input signal
fft_inp = fft(input);
```

```
% Finding the Fast Fourier Transform of the output signal
fft_out = fft(output);
% Obtaining the transfer function frequency response. This is an
array of
% complex numbers
tf = fft_out./fft_inp;
% Obtaining the phase angle plot of the transfer function repre-
sented by 'tf'
ang(1:final) = angle(tf(1:final))*180/pi;
% Converting angles in the range 160 - 180 to -180 - -200
for i = 1:final
    if ang(i) > 160
        ang(i) = ang(i) - 360;
    end
end
```

A.2 SYSTEM EVALUATION AND CHECK FOR CYBER ATTACK

```
%%%%%%%%%%%%%%%%%%%%%%%%%     MAIN_CASE
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Time of which the simulation is run in SimuLink
n = 200;
% Time step used
T = 0.01;
% Finding the sampling frequency
Fs = 1/T;
% Finding the total number of signal values
L = n*Fs;
% Finding the mid point so that the second half of the fourier
transfer can
% be ignored
h = L/2+1;
% Generating the frequency array corresponding to which the
phase angles will
% have to be plotted
f = Fs/2*linspace(0,1,h);
% Converting the frequency from Hertz to radian per second
f = f*2*pi;
% Finding the maximum phase angle differences and the frequen-
cies at which
% they occur for each of the six transfer functions
[max_diff1,frequency1] = phase_comparison (c,a,initial_ang1,f);
[max_diff2,frequency2] = phase_comparison (c,r,initial_ang2,f);
[max_diff3,frequency3] = phase_comparison (c,b,initial_ang3,f);
[max_diff4,frequency4] = phase_comparison (c,d,initial_ang4,f);
[max_diff5,frequency5] = phase_comparison (r,b,initial_ang5,f);
[max_diff6,frequency6] = phase_comparison (e,d,initial_ang6,f);
% Forming an array with maximum phase angle differences observed
in all six
% different transfer functions
max_difference = [max_diff1 max_diff2 max_diff3 max_diff4
max_diff5 max_diff6];
% Forming array containing the frequencies at which the maximum
phase angle
% differences occur in each of the six transfer functions
frequency = [frequency1 frequency2 frequency3 frequency4 fre-
quency5 frequency6];
% Initializing the flag matrix
flag = zeros(5,6);
% Modifying the flag matrix depending on the tolerance matrix
and the maximum
```

```
% phase angle difference array
for i = 1:5
    for j = 1:6
        if max_difference(j) > tolerance(i,j)
            flag(i,j) = 1;
        end
    end
end
% Forming the row sum matrix that finally depicts if there is a
cyber attack
% in the system or not
row_sum = flag*[1; 1; 1; 1; 1; 1];
% Displaying if a cyber attack is detected
for i = 1:5
    if row_sum(i,1) == 6
        fprintf('CYBER ATTACK DETECTED!!\n');
    end
end
%%%%%%%%%%%%%%%%%%%%%%%%     PHASE_COMPARISON
%%%%%%%%%%%%%%%%%%%%%%%%%%
% Function used to obtain the maximum phase angle differences
between the
% phase angle plots of the transfer functions in the current
system condition
% and the base system phase angle plots
% max_difference - Maximum phase angle difference between the
phase angle
%                  plots of the transfer functions in the base
case and the
%                  current case
% frequency - Frequency at which the maximum phase angle differ-
ence occurs
% input - input signal array
% output - output signal array
% initial_ang - phase angle plot of the transfer functions in
the base case
% f - Frequency array
function [max_difference,frequency] = phase_comparison (in-
put,output,initial_ang,f)
% Starting frequency of 2 rad/s
initial = 65;
% Ending frequency of 20 rad/s
final = 650;
% Finding the Fast Fourier Transform of the input signal
fft_inp = fft(input);
```

```
% Finding the Fast Fourier Transform of the output signal
fft_out = fft(output);
% Obtaining the transfer function frequency response. This is an
array of
% complex numbers
tf = fft_out./fft_inp;
% Obtaining the phase angle plot of the transfer function repre-
sented by 'tf'
ang = angle(tf)*180/pi;
% Converting angles in the range 160 - 180 to -180 - -200
for i = 1:final
    if ang(i) > 160
        ang(i) = ang(i) - 360;
    end
end
% Finding the phase angle differences at frequencies 2 rad/s to
20 rad/s
for i = initial:final
    difference(i) = abs(ang(i) - initial_ang(i));
end
% Rejecting phase angle differences of over 20 degrees
for i = initial+1:final
    if difference(i) > 20
        difference(i) = difference(i-1);
    end
end
% Finding the maximum phase angle difference in the frequency
range of
% 2 rad/s to 20 rad/s. Also finding the frequency at which this
maximum
% phase angle difference occurs.
[max_difference,index] = max(difference);
frequency = f(index);
```