IMPACTS OF TIME DELAY AND FALSE DATA INJECTION ATTACKS ON POWER SYSTEM CONTROL LOOPS

By

SAI LALITHA DATTATREYA POOSARLA

Bachelor of Science in Electrical Engineering

JNT University Kakinada

Andhra Pradesh, India

2015

Submitted to the Faculty of the
Graduate College of the
Oklahoma State University
in partial fulfillment of
the requirements for
the Degree of
MASTER OF SCIENCE
July 2017

IMPACTS OF TIME DELAY AND FALSE DATA INJECTION ATTACKS ON POWER SYSTEM CONTROL LOOPS

Thesis Approved:

Dr. Yuanxiong Guo

Thesis Adviser

Dr. Ekneligoda

Dr. Gary Yen

ACKNOWLEDGEMENT

I sincerely thank my graduate advisor Dr. Yuanxiong Guo for his encouragement, guidance, and support throughout this research. It is his way of teaching that made me think of the concepts in a different way and made me dig deep into the subject and come up with ideas and solutions. I thank my thesis committee members, Dr. Gary Yen and Dr. Nishantha Ekneligoda for their valuable suggestions and constant encouragement towards completion of my thesis.

I would like to take this opportunity to thank my friends and others for their love, support, and encouragement. They have always encouraged and helped me refine the way to think about things & ideas and not to lose my confidence.

Finally, I thank my parents, brother and my family members for their unconditional love and constant support throughout my life who encouraged me to move to US for pursuing a good career in the field of Power and Renewable Energy.

Name: SAI LALITHA DATTATREYA POOSARLA

Date of Degree: JULY, 2017

Title of Study: IMPACTS OF TIME DELAY AND FALSE DATA INJECTION ATTACKS ON POWER SYSTEM CONTROL LOOPS

Major Field: ELECTRICAL ENGINEERING

Abstract: Modern power grid is one of the largest cyber-physical infrastructure seen in our daily life. Wide-Area Monitoring, Protection and Control System (WAMPCS) ensures that the power grid operates in a stable condition by allowing real-time remote control and measurement over the power grid. Apart from this, WAMPCS, because of the extensive use of IT infrastructure exposes the system to potential cyber attacks. In this thesis, impacts of some of these attacks; time delay attack (TDA), false data injection attack (FDA) on the frequency and voltage control loops are analyzed. To analyze the effects on frequency control loop an identical 2 area tie-line system is considered. The characteristic equation of the system under TDA is used, to determine the optimum value of delay that brings the system to marginal stability. Similarly, the range of FDA proportional constant (ε), that keeps the system in stable condition is determined using the characteristic equation of the system under FDA. Likewise, the effects on voltage are studied on an IEEE excitation loop which comprises the basic components for terminal voltage control in a generator excitation system. An analysis similar to the frequency control loop is made and the characteristic equations for the system under the two attacks are developed. Optimum values for the time delay and the range of FDA proportional constant (ε) for the system stability are obtained. Results have shown that the system does not go into instability if the attack parameters values lie in the determined range. Any value other than that moves the system towards instability. Also, it is observed that in either control loops a combined attack is more powerful than when an attack is launched individually. Considering the effect of power market on system performance, mitigation strategies for the attacks can be integral parts of future work to improve protection for the power system.

TABLE OF CONTENTS

LIST OF TABLES

Table Page

LIST OF FIGURES

Figure Page

CHAPTER I

TRADITIONAL AND MODERN POWER SYSTEM

Power System consists of 3 main components (i) Power Generation system (ii) Transmission system (iii) Distribution system. Precisely, the function of the traditional power system can be summarized as the power generation is the place where the power required by the customers is produced and supplied to the customers through the distribution lines at the user consumable voltage. Transmission lines are used to carry the power from the generation station to the distribution substations at higher voltages to reduce the power loss in the transmission process. Then the power is transferred from the distribution substations to the end users, simply called the distribution system.

1.1. **Traditional Power System**

Traditional Power System has been very old and needs to be updated. In most of the Power Systems of the world, the T&D is a vital link between generating stations and the customers. Aging equipment and growing demand have been stressing the system making it more prone to blackouts. So, there is an urgent need for the modernization of our power system. Electrical power reliability and economy have proven to be one among many factors for the modernization of the society. Inadequate investments in T&D system to meet the increasing demands, limited availability for the accommodation of renewables into the system which produces the energy intermittently have made the system face major vulnerabilities.

Moreover, significant utilization of the renewable generators placed far away from the loads cannot be achieved until there are significant reserves connected to the transmission system. Also, Distribution Systems are generally incompatible with demand side management which is an economical way of energy conservation. But modernization of the T&D system could eliminate these problems. US T&D system is regarded as the greatest engineering achievement of the 20th century in the US.

T&D are two distinct systems which are strongly connected to each other.

a. Transmission System is that part of the power system that helps in transmitting the power generated from the generation plants to the substations. The transmission voltages are generally of the high range of about 230kV-765kV. Transmission systems are generally interconnected and therefore the power has multiple paths to move from generator to the distribution substation.
b. The distribution system is that part of the power system which helps in the transmission of the power from the distribution substation to the consumer terminal. This system generally operates at low voltages and unlike transmission system is mostly radial which makes the system suitable for power flow only in one direction.

Current US electrical transmission system can be divided into 9 ISO's, where each ISO is responsible for maintaining the system reliability and economical dispatch of the electrical power in their regions maintaining the load generation balance & monitoring the power flows in the transmission lines.

The Fig.1.1. shows Independent System Operators and Regional Transmission Organizations in the US. Colored regions indicate that there has been a change in the structure of the power industry. Non-colored regions indicate that the region has an only vertical transfer of power from generator plants to consumer.

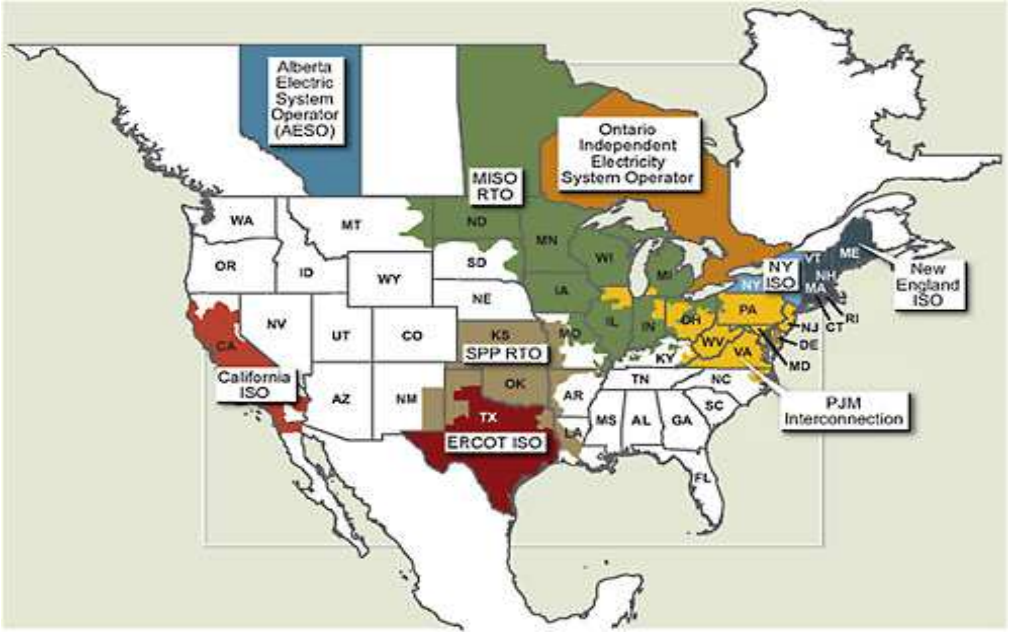

Figure 1.1. Independent System Operators of USA

Source: https://www.nap.edu/read/12091/chapter/13

Operationally, entire US& Canada is divided into 4 interconnections. The Quebec Interconnection is shown as part of the Eastern Interconnection because operations are coordinated. Technological evolution, environmental policies, expansion of finance into the field of electrical markets altogether encourage the promotion of new conditions for the sector of power generation. New advancements permit the power to be created in little-estimated plants. New technologies provoke the power production in small scale plants. Additionally, the expanding utilization of renewable sources keeping in mind the end goal to diminish the natural effect of force era prompts to the improvement and use of new electrical vitality supply schemes. In this concept, power is not generated only in level 1. Therefore, the energy demand is not only supplied by the centralized generator but also a part of the load is supplied by the distributed/renewable generators, which means electricity is produced near to the consumers.

1.2. Modern Power System

Because of changing IT infrastructure and modern technologies for power generation the power is not being generated at the centralized locations but also on the distribution side. This requires more communication requirements from the distribution side to the generation side as well from the generation to distribution side. Some of the major components of the modern power system are

1.2.1 Distributed Generation

Different definitions for Distributed Generation(DG) are being used in practice in literature and practice. Terms like decentralized, dispersed generation are other words commonly used instead of Distributed. DG can generally be defined as the production of power at the points of consumption. Generating power on-site rather than at the center eliminates the requirement of transmission power from far distances thereby reduces the losses in the system. Ackermann defined Distributed Generation ‘as a power source that is connected to the distribution network of the meter side of the power network. Wide varieties of technologies are used for the development of the new technologies.

Another classification of DG is the type of fuel they use- fossil fuels or non-conventional energy source. The type of primary source decided the type of connection to the grid. Based on output characteristics DG can be termed as dispatchable and non-dispatchable. The DSO can be able to dispatch the DG output by controlling the amount of input fuel given to the DG. When it is not dispatchable the DSO has no way to control the outputs of the DG. These systems generally use renewable energy resources as their fuel. There are many DG technologies currently available such as Solar power, wind power, cogeneration, hydropower, waste to energy, energy storage.

1.2.2. Microgrid

A localized group of electrical generation, energy storage, and loads normally connected to the main grid (macro grid). The microgrid can function autonomously without the main grid. It has a connection switch for the connection to the main grid, under necessary conditions this microgrid can be used to supply as well as take power to or from the main system thereby maintaining the reliability of the system. Generation and load in microgrid operate either in DC/AC or a combination of both. Recent developments in renewable energy systems, storage, and new emerging load natures are being used by the researchers for the comparison of performance and efficiency of ac grids with the dc grids.

The general generators used in the microgrids are stationary batteries, solar, wind, biomass or other energy sources. Multiple distributed generators and isolation of the microgrid from the main grid increases the reliability of electric power. Heat produced from the microturbines can be used for local process heat or space heating after sufficient trade-off between the heat requirement and electrical power requirement has been made. A basic microgrid has small power stations of 5-10 MW to serve the grid, cover a radius of 30-50km, generate power locally to reduce the dependence long transmission lines. Fig.1.2 shows Sendai microgrid at Fukushi in Japan.

Figure 1.2. Microgrid at Fukushi, Japan

1.2.3. Energy Storage

Energy storage is the capture of energy produced at one time for use at later time. The device that stores this energy is called an accumulator. Energy storage involves the conversion of energy from the inconvenient storable forms to the storable forms. Bulk storage is possible through pumped hydro plants. Some technologies store the energy only for a short period whereas few store for long periods of time. The major components of energy storage system are

i. Charging System: Method of sending the energy system from external system to storage system
ii. Storage Medium: The device which will store the energy until it is required
iii. Discharging Medium: The method of releasing the stored energy into the power system
iv. Control: Controlling the operation of charging and discharging operation of the energy storage system.

Different energy storage technologies can be classified depending on

a) Type of extraction:
    i) Direct Extraction
    ii) Indirect Extraction
b) Time Domain Response Characteristics
    i) Short term storage: The time generally varies from seconds to minutes and is used for power quality applications
    ii) Long Term Energy Storage: This term varies from minutes to hours, used in frequency response & grid congestion management
    iii) Real Long Time Storage: The term of operation varies from hours to days, Used for supply demand matches for long periods of time.

c) The medium of Storage:

i) Mechanical

ii) Electrical or Magnetic

iii) Chemical

iv) Thermal

Advantages using the energy storage devices in the distribution system are

i) Integration of power through renewable energy resources: Energy storage systems help in reducing the negative effects of renewable generators like intermittency. In order to quickly react to the changes, it is necessary to employ systems with high lifetime and short response time. Therefore, super-capacitors, batteries, and SMES are therefore suited for this purpose.

ii) Load shifting: The energy stored in the storage systems can be used to supply the energy when the generation is unable to cope up with the load or these storage devices can be used to absorb the excess energy during the off-peak hours thereby shifting the energy used from off-peak to peak hours. This helps in smoothening of excess grid demand with good penetration of renewables.

iii) Voltage/VAR Support: The storage systems are associated with the inverters that can be used for the production of required amount of reactive power, to maintain the voltage in the system.

1.2.4. Smart Meters

Smart meters are the electronic devices that are used to record the consumption of electrical energy in terms of hours/less and communicates this information to the utility at least once a day for making up the utility for monitoring and billing. Unlike traditional meters, smart meters have the capability of two-way communication that enables it to send the information to the utility and also get the information from the utility company. The smart meters not only measure the amount of power being consumed but also helps in monitoring the power quality and sends the power outage

notifications to the utility. These meters are also referred to as 'Advanced Metering Infrastructure' (AMI) meters.

Potential benefits of using the smart meters are:

i) These meters pit an end to the estimated bills, which are a major source of complaint

ii) It can help consumers regulate their power usage thereby managing their bills

iii) Demand side management & load shifting practices can be easily achieved using the smart meters as the customer would know the time of peak usage of power when the unit electricity cost would be higher this encouraged the customer to minimize his load during peak hours and shift it to hours of low demand.

Challenges of using smart meters:

i) Meters must have reliable and secure communications with the central utility for transmitting the collected information

ii) Privacy is of a major concern since the electricity usage can tell a lot of information about the home, secure transmission of the data is a major issue.

Fig.1.3. Shows a brief view of the modern power system consisting renewable power generation sources, IT communication network, microgrids and smart meters.

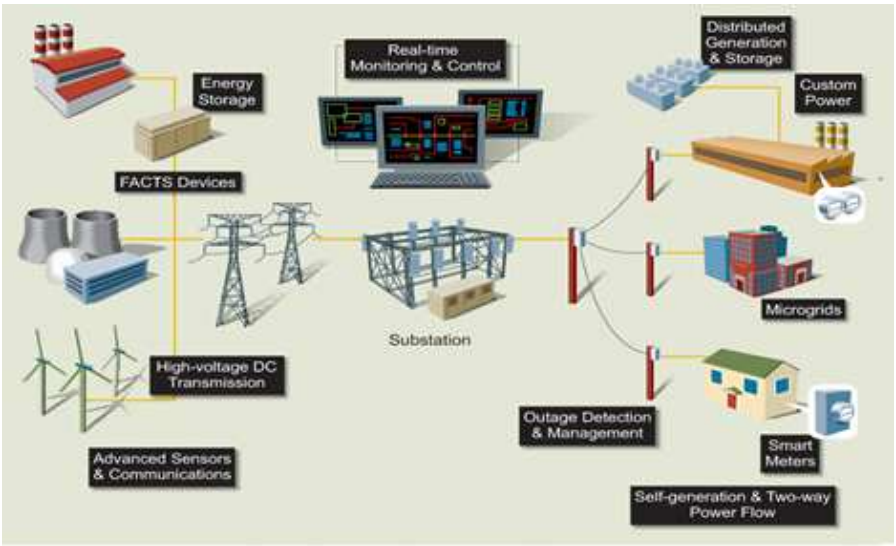

Figure 1.3. Modern Power System

CHAPTER II

CONTROL LOOPS IN POWER SYSTEMS

Having studied about the traditional and modern power system, we now know that there is a lot of IT infrastructure involved in the modern power system. In this chapter we will study about the major control loops present in the modern and traditional power system, having the possibility of being attacked by any cyber intruder, to destabilize the system.

As the major goal of the power system is to supply secure and reliable energy to the customers. There are two major parameters that assess the quality of the power supplied

i. Voltage

ii. Frequency of the power supplied

Therefore, in order to achieve a higher quality of operation, these system parameters are associated with feedback control loops. These loops form the major automatic control loops in power system. Because of their extreme importance in the quality assurance, there is always a possibility of threat for the proper operation of the system.

2.1. Voltage Control Loop

For reliable operation of power system, the voltage and reactive power control should satisfy the following objectives

a. The Voltage at the terminal ends of all equipment in the system should be within the voltage

limits, utility and customer equipment are always designed to operate at a certain range but the prolonged operation of equipment outside the range damages the equipment.

b. Regulate the reactive power flow in the transmission lines to reduce the active and reactive power loss in the transmission system.

The task of regulating the voltage in a vast power system is very difficult because it has a number of loads and generator units. As the loads vary the reactive power requirement for the system varies. Since the reactive power cannot be transmitted over long distances, voltage control needs to do at regular places using special devices. Proper selection and coordination of equipment for controlling reactive power and voltage are major challenges in the power system engineering.

Some of the devices used for the reactive power control in the power system are synchronous generators, transmission lines, underground cables, static var compensators, shunt capacitors, shunt reactors, etc. Fig 2.1 depicts a standard voltage control loop defined by IEEE system in the excitation system.

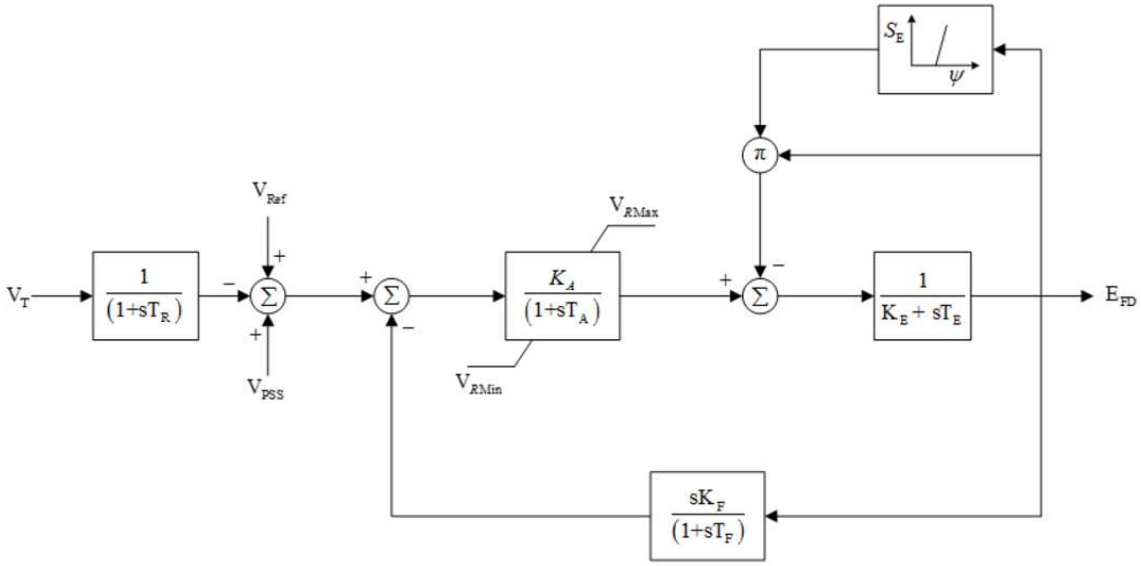

Figure 2.1 IEEE defined basic Excitation system

Where T_R, T_A, T_E, T_F: Transducer, AVR, Exciter, Feedback time constants

and K_A, K_E, K_F : AVR, Exciter, Feedback Gain constants.

2.2. Frequency Control Loop

For satisfactory operation of power system, the frequency should be maintained at fairly constant value. Relatively close control of frequency ensures the working of synchronous and induction motors at constant speeds. The constancy of the speed of these drives good performance of the auxiliary systems on which are dependent the fuel, water feed and combustion air supply streams. In a system with a considerable drop in frequency can cause the high flow magnetizing current in the system causing more losses.

The frequency of the system depends on active power balance in the system. Since frequency is a common factor throughout any change in load at any point in the power system leads to frequency disturbance. Since Power system has many generators, the primary control loop i.e the speed governor provides the primary speed control of the generators and the secondary control loop allocates the change of loads to the generators in the system.

In an interconnected system along with control of frequency, the tie-line power flow between the controlled areas must also be set to the scheduled values. This control of generation and frequency is referred to as load frequency control (LFC).

The basic components of the load frequency control loop are

i. Governor

ii. Prime Mover

iii. Generator & Load

iv. AGC system

The above components can be explained briefly as

i. Governor: If a generating system is operating with constant mechanical input and there is a sudden change in load and if the mechanical input to the generating system does not change then

the frequency of the system moves far away from the operating value. In order to avoid such kind of situation a governor is used, it senses the mechanical input to the generation system and then adjusts the valve from in such a manner that the mechanical energy is changed either increased/ decreased to meet the system load and bring back the frequency to its nominal value. The block diagram representing a Governor is shown in Fig 2.2.

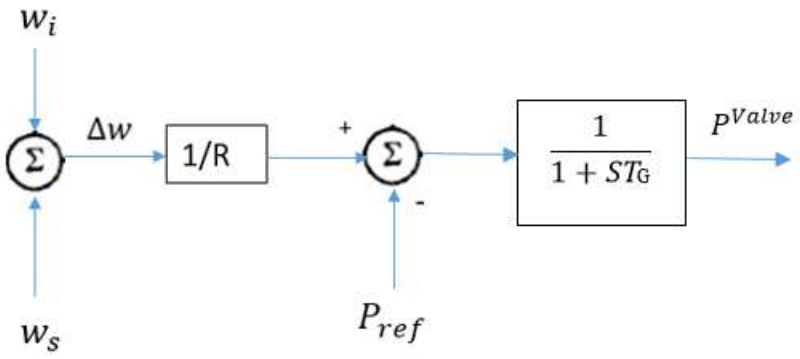

Figure 2.2 Governor Block

T_G: Governor time constant

ii. Prime Mover: Prime mover driving the generator unit is generally a steam or hydro turbine. This is the model that converts the potential energy into mechanical energy. The models for the prime mover must take into account steam and boiler control characteristics for steam turbine and penstock characteristics for a hydro turbine. But for basic analysis model for the non-reheat turbine is sufficient. This model can be represented as depicted in Fig. 2.3.

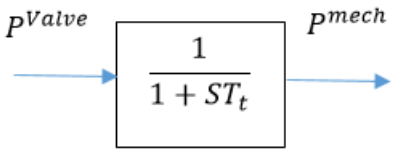

Figure 2.3 Turbine Block

T_t: Turbine time constant

iii. Generator and Load: The swing equation of the generator can be used to get the basic model for the load system. The swing equation describes the relation between the electrical power, mechanical power and the speed of the generator. It is given as

$$\frac{dw_i}{dt} = -\frac{D_i}{M_i}w_i + \frac{1}{M_i}P_i^{mech} - \frac{1}{M_i}P_i^{elect} + \frac{D_i}{M_i}w_s$$

M_i-Inertia of the synchronous generator

D_i- Damping coefficient of the generator

w_i- angular speed of the generator

Since the power system consists of different types of loads e.g. constant power, constant current, frequency depended load. If frequency depended load is considered to be existing in the system Then if d=$\Delta w_i/\Delta P_L$, the transfer function and the corresponding block diagram for the generator load system is as shown in Fig.2.4.

$$\frac{\Delta w_i(S)}{(P_i^{mech}(S) - P_i^{elect}(S))} = \frac{\frac{1}{M_i}}{(S + \frac{(D_i + d)}{M_i})}$$

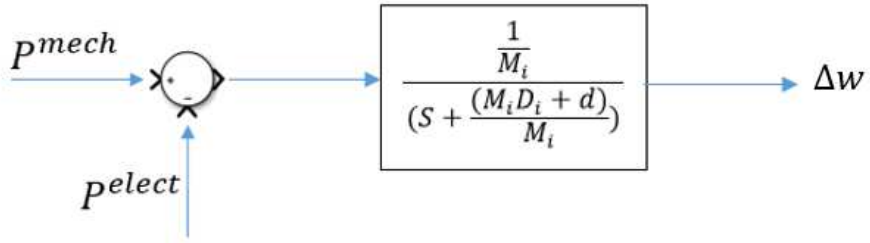

Figure 2.4. Generator and Load Model Block

iv. AGC System: This is the secondary control loop in the power system having 2 major objectives

a. Maintain the frequency of the system at nominal frequency

b. Maintain the tie line power to scheduled values

In order to achieve these objectives, an error called the area control error is given as the input to this secondary control loop that helps to reduce this error and maintain the system at a constant frequency and maintain scheduled tie line power flows. Fig. 2.5 shows the block diagram satisfying all the objectives of the automatic generation control.

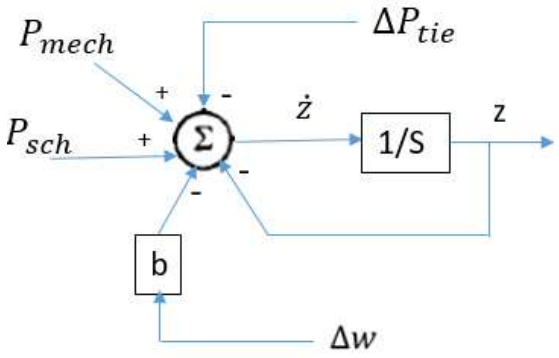

Figure 2.5. Automatic Generation Control Block

CHAPTER III

MOTIVATION FOR CYBER-PHYSICAL SYSTEMS

3.1. Motivation

In this chapter, we introduce the motivation for the requirement of assessment of the system performance for the uncertainties arising from physical and cyber components of the power system. Since current power systems are undergoing radical transformations for improving reliability, environmentally friendly generating systems and have better economic operations, emerging technologies such as renewable generation, advanced cyber communication infrastructure and demand response resources can lead to the introduction of new sources of uncertainty. This causes new challenges to the operation and performance of power system. In this thesis, we study the impact of cyber-attacks on power system performance and identify the critical values for the attack parameters which makes the system unstable.

Cyber-Physical Uncertainty Impact: There is a special attention towards the communication network protocols of the power system in the vision of smart grid. Supervisory Control and Data Acquisition systems (SCADA) is a computer controlled system that has been widely used in the monitoring, control, and protection of power system. DNP3 is the distributed network protocol that is used for SCADA systems in power network. Due, to the lack of authentication of SCADA communication protocols it is always possible for the intruders to attack the system and

manipulate the data in the SCADA systems. The attacks or data manipulation could be in the form of delaying the measured signal, delay sensor output, inject false data/commands, denial of service attacks etc., Many techniques have been developed in order to detect the attacks based on the State Estimation (SE). Nevertheless, there is also a lot of research done to attack the SE. Since one of the inputs to the AGC is from this measured signals the integrity of frequency measurement is difficult to be ensured. Also, the developing communication infrastructure made the wide area measurement systems (WAMS) available for understanding and managing the complex behavior of the power system. Advanced metering devices, Phasor Measurement Units (PMUs) measures both the magnitude and phase angles of the voltages with high sampling rates at places with ≥ 200kV. The protocol for the synchrophasor communication has been given by the IEEE standard, which tough can be manipulated by spoofing the synchronized clocks in PMU's.

Both the protocols DNP3 and synchrophasor communication protocols belong to the application layer and suggest Ethernet with TCP/IP, lower layers of the communication network. However, these TCP/IP protocols are not designed for networked control systems, therefore there is a greater possibility for the system to be attacked. Also, there is an arousal of unavoidable noise in the system because of this communication protocols.

For the analysis of impact, we concentrate on the AGC system, as it is the only automatic control loop in the power system that is dependent on IT infrastructure. Since AGC takes the measured data such as frequency, power flow between the balancing authorities as inputs and sends the control decisions for the amount of power generation from the generators through IT infrastructure, the system gets damaged if there is any intrusion in the communication system.

Looking from the AGC's perspective, though AGC has been used since decades there is a considerable interest in re-examining the AGC system's performance with various new techniques of power system operation and control. Traditionally, it is assumed that the operation time of the

AGC system is far more than any other component of the power system, as a result, it has always been neglected for the dynamic system analysis. However, this assumption is no longer true because of the increased number of power plants having larger inertia. Furthermore, new generating plants challenge the operation and performance of AGC. For example, high penetration of renewable energy sources into the power system increases the variability in the system and can potentially lead to the failure of AGC system. Also, because of new ancillary service market resources such as batteries, temperature controlled loads etc., can add a lot to the variability in the power system. Therefore, the AGC system needs to be considered while studying the dynamics of the power system, and system dynamic simulations that include this AGC model needs to be developed.

3.2. Broader Classification of Cyber Attacks

Uncertainties faced by the power system can be classified into 2 types

i. Aleatory - Objective and inherent uncertainty

Some of the sources of this uncertainty are

- Failures and Repairs of cyber and physical equipment
- Renewable generation sources whose generation is difficult to be predicted
- Unpredictable behavior of DRRs
- Uncertainties in economic policies of fuel and raw energy prices market information.

ii. Epistemic – Subjective uncertainty

This can be explained as the difference between the measured values and estimated values arising because of an unclear understanding of the scientific behavior of the underlying process. These arise from

- Parameters in the dynamic and static models describing any system

- Errors arising from the measuring devices because of the malfunction and malicious cyber attacks.

3.3. Literature Review

Among various cyber attacks existing we analyze the effect of (i) Time delay attack and (ii) False data injection attack in the AGC loop of the power system. To this end, we develop the block diagram for the power system with AGC in Simulink. In this section, we review the existing related work and see the look at the gaps that need to be analyzed.

3.3.1. Impact of Measurement Uncertainty

As mentioned earlier, safe transfer of measurement signals from the power system to the control unit is an important task for maintaining the reliability of the operation and control of the power system. However, malfunction and noise intrusion into the transmitting signal is an inevitable phenomenon. Therefore, the measurement data is prone to cyber attacks which introduce engineered errors and can lead to the degradation of the power system. Flaws in the power system due to cyber attacks have been heavily documented [2]; therefore, it is necessary to summarize the different types of measurement uncertainties. In terms of the types of measurement uncertainty, measurement data can be delayed, manipulated or even lost. Example, for the delay, can be due to excessive communication traffic or denial of service attacks [3], [4]; Manipulation e.g., due to man-in-the-middle attacks, see [5]; Lost (e.g., through a lossy network, see [6], [7]).

In this thesis, we focus on the impact of measurement errors and delays.

Impact of Measurement Errors: Depending on the required purpose, measurements can be manipulated in a number of ways and numerous research has been done in this field. For instance, [8] explains the class of FDI attacks that can manipulate the estimated system state in an arbitrary way. [9] Presents the impact of measurement errors on the power market. In [10] the authors explored the impact of integrity attack on the measurements for AGC to mislead the operator to perform incorrect control operations thereby triggering the wrong actions like generator isolation,

load shedding etc., leading to sequential failures. However, there is very less work done on studying the effects of measurement errors on system dynamic performance.

Impact of Measurement Delays: Measurement delays too can be of different forms. [11] considers a system where the delays are taken from a finite set and then the stability of the system is studied. [12] studied the stability of a real-time control system with random delay input having zero mean as an attack. [13] measured experimentally the effect of delay errors in Ethernet-based communication infrastructure for power systems. [14] explored the effect of communication delays on the electricity market. However, there is only a small research work is going on studying the impact of delay errors on dynamic studies of the power system.

3.3.2. Real Time Cyber attack on Ukrainian Power grid

On 23rd December 2015, Ukrainian Kyivoblenergo, a regional electric utility company reported outages to the customers. The attack basically took place because of the intrusion by a third party people into the company's SCADA systems and computers. The attack started at around 3:35 pm when 7, 110kV and 23, 35Kv substations were disconnected from the distribution grid. Later, the existence of the other effects came into the picture and forced the operators to switch to the manual mode. The investigation has later proved that the attack was caused by a foreign attacker who intervened with the SCADA system of the distribution management system. It was originally assumed that the effect has affected 80,000 customers, however, later it was revealed that the attack was launched on 3 different energy distribution companies at the same time affecting approximately 225,000 customers losing power across various areas [15] [16].

Shortly after the attack, the Ukrainian government has claimed that the attack to be launched by the Russian security services, as there was a war going on between Ukraine and Russia at that time [17]. Taking these claims into consideration investigators of Ukraine, U.S Government and some

private companies performed analysis and offered their support to determine the root cause of the outage.

These cyber attacks in Ukraine are the first attacks that caused the power outage to the public. As future attacks can take place with greater possibility, it is important to study and understand the sources and impacts of these attacks. The extent of the damage because of a power outage is measured in terms of a number of customers affected, the amount of electrical energy wasted and electricity infrastructure involved and time is taken for the restoration. Analysts said that a similar attack launched in the USA can probably lead to a greater damage because of its excessive usage of IT infrastructure in its electrical network.

CHAPTER IV

EFFECTS OF CYBER ATTACKS ON FREQUENCY AND VOLTAGE CONTROL LOOPS IN POWER SYSTEM

4.1. Frequency Control Loop

As we know that there are a number of components involved in the frequency control loop in this chapter we develop the mathematical expressions defining the functioning of the elements. Also, we would develop mathematical expressions for the cyber attacks and see the effect of the system stability for changing values of the cyber attack parameters.

In order to maintain the system under stability, the supervisory control and data acquisition (SCADA) system act centrally (i.e. control center) for implementation of AGC algorithms. AGC system is required for (i) regulating frequency (ii) regulate the tie line power between balancing authorities at scheduled values. In order to satisfy these objectives, the AGC system takes the measurements of (i) area frequency (ii) output power generated from the committed units (iii) interchange power flowing between the balancing areas. Then the AGC system calculates the area control error (ACE) and calculates the new generator set point values by driving the ACE to zero. All the measurement signals and control commands are received and sent to various points over the cyber network. It is then apparent that the measurement data is critical for proper functioning of the system and any misleading data in AGC algorithm can affect the performance of the system and make the system unstable. Therefore, the modeling framework adopted in the thesis

considers the standard power system electromechanical dynamics model. This chapter also includes the modeling of all the components that form the frequency control loop of the power system.

4.1.1. Mathematical Modelling of Components in Frequency Control Loop

4.1.1.1 Generator & Load Block

Swing equation is that which describes the relationship between the frequency deviation of the generator, mechanical and electrical powers. (4.1) gives the mathematical equation for the swing, rearrangement and applying the Laplace transform, converts (4.1) to (4.5)

$$\frac{dw_i}{dt} = -\frac{D_i}{M_i}w_i + \frac{1}{M_i}P_i^{mech} - \frac{1}{M_i}P_i^{elect} + \frac{D_i}{M_i}w_s \tag{4.1}$$

$$\frac{d\Delta w_i}{dt} = -\frac{D_i}{M_i}\Delta w_i + \frac{1}{M_i}(P_i^{mech}(S) - P_i^{elect}) \tag{4.2}$$

where w_i-w_s= Δw_i

Applying the Laplace transform

$$S\Delta w_i(S) = -\frac{D_i}{M_i}\Delta w_i(S) + \frac{1}{M_i}(P_i^{mech}(S) - P_i^{elect}(S)) \tag{4.3}$$

$$\Delta w_i(S) = \frac{1}{M_i}\frac{(P_i^{mech}(S) - P_i^{elect}(S))}{\left(S + \frac{D_i}{M_i}\right)} \tag{4.4}$$

$$\frac{\Delta w_i(S)}{(P_i^{mech}(S) - P_i^{elect}(S))} = \frac{\frac{1}{M_i}}{(S + \frac{D_i}{M_i})} \tag{4.5}$$

M_i-Inertia of the synchronous generator

D_i- Damping coefficient of the generator

w_i- angular speed of the generator

a. If damping of the machine is assumed negligible, then $D_i = 0$ and (4.5) transforms to (4.6)

$$\frac{\Delta w_i(S)}{(P_i^{mech}(S) - P_i^{elect}(S))} = \frac{1}{M_i S} \tag{4.6}$$

b. If frequency depended load is considered in the system, then if d=$\Delta w_i / \Delta P_L$ the transfer function for the generator block is given by (4.7)

$$\frac{\Delta w_i(S)}{(P_i^{mech}(S) - P_i^{elect}(S))} = \frac{\frac{1}{M_i}}{(S + \frac{(D_i + d)}{M_i})} \tag{4.7}$$

4.1.1.2. Governor Block

As the governor tries to regulate the mechanical input to prime mover the output of the governor block is P_{mech} and takes input of reference power P_{ref}. Time domain and Laplace domain equations describing the Governor block are given by (4.8) and (4.11) respectively

$$\frac{dP_i^{mech}}{dt} = -\frac{1}{\tau_i R_i} w_i - \frac{1}{\tau_i} P_{mech} + \frac{1}{\tau_i} P_i^{ref} + \frac{1}{\tau_i R_i} w_s \tag{4.8}$$

Applying Laplace Transform

$$SP_i^{mech}(S) = -\frac{1}{\tau_i R_i} \Delta w_i(S) - \frac{1}{\tau_i} \left(P_i^{mech}(S) - P_i^{ref}(S) \right) \tag{4.9}$$

$$\left(S + \frac{1}{\tau_i} \right) P_i^{mech}(S) = -\frac{1}{\tau_i R_i} \Delta w_i(S) + \frac{P_i^{ref}(S)}{\tau_i} \tag{4.10}$$

$$P_i^{mech}(S) = \frac{-\frac{1}{\tau_i R_i} \Delta w_i(S) + \frac{P_i^{ref}(S)}{\tau_i}}{\left(S + \frac{1}{\tau_i} \right)} \tag{4.11}$$

τ_i- Time constant of the Governor

R_i- Governor regulation constant (slope of governor droop graph)

w_s- Synchronous speed of the generator

P_i^{ref} - Set point value for the generator

A turbine block can be modeled as complex as required by taking more number of reheating spots in turbines. So, a simple first order model of a turbine is taken for the analysis.

4.1.1.3. AGC Block

So the main aim of AGC block is to make area control error ACE to zero. So, the ACE is calculated and is integrated over time i.e. given to a PI controller to make the error go to zero. ACE is calculated from (4.12)

$$ACE = \beta\Delta f + \left(P_{tie} - P_{tie}^{Sch}\right) \tag{4.12}$$

The AGC algorithm gives the new set point values for the generators as the output which can be modeled by (4.13). The Laplace transformed AGC system dynamics are given by (4.15)

$$\frac{dz_m}{dt} = -z_m - ACE_m + \sum Pg_m \tag{4.13}$$

$$Sz_m(S) = -z_m(S) - \left(P_{mn}(S) - P_{mn}^{Sch}(S)\right) + b\left(\Delta w_i(S)\right) + \sum P_{mech}(S) \tag{4.14}$$

$$z_m(S) = \frac{1}{S}\left(-z_m(S) - \left(P_{mn}(S) - P_{mn}^{Sch}(S)\right) + b\left(\Delta w_i(S)\right) + \sum P_{mech}(S)\right) \tag{4.15}$$

Where z_m- Sum of set point values for the generators participating in AGC in an area m

P_m^g- Current active power generation from the generators participating in AGC

4.1.1.4. Tie Line System

Since the power system is very huge it is divided into a number of sub-areas called the balancing areas. For the simplicity, we can model the power flowing in these lines by their equivalent DC power flow equation, which is given by (4.16)

$$\Delta P_{tieflow} = \frac{1}{x_{tie}}(\Theta_1 - \Theta_2) \tag{4.16}$$

(4.16) can be represented in integral form as in (4.17)

$$\Delta P_{tieflow} = T \int (w_1 - w_2)\, dt \tag{4.17}$$

Where T=377/x_{tie} for a 60 Hz system

Applying Laplace Transform to tie-line power flow equation, (4.17) gives (4.18)

$$\Delta P_{tieflow}(S) = \frac{T}{S}\big(\Delta w1(S) - \Delta w2(S)\big) \tag{4.18}$$

Where Θ_1, Θ_2 - Voltage angle at bus 1 and 2 connecting the BA connected by tie-lines.

Combining all the blocks of frequency control loop gives the single area system as shown in Fig. 4.1. Considering the combination of two identical areas connected by tie lines gives the load frequency control loop for a 2 area system shown in Fig. 4.2.

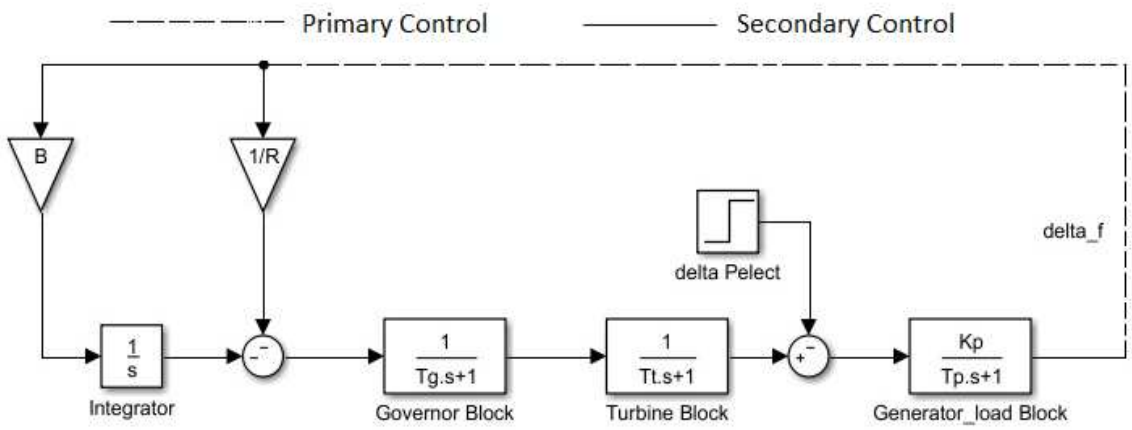

Figure 4.1. Single area load frequency control loop

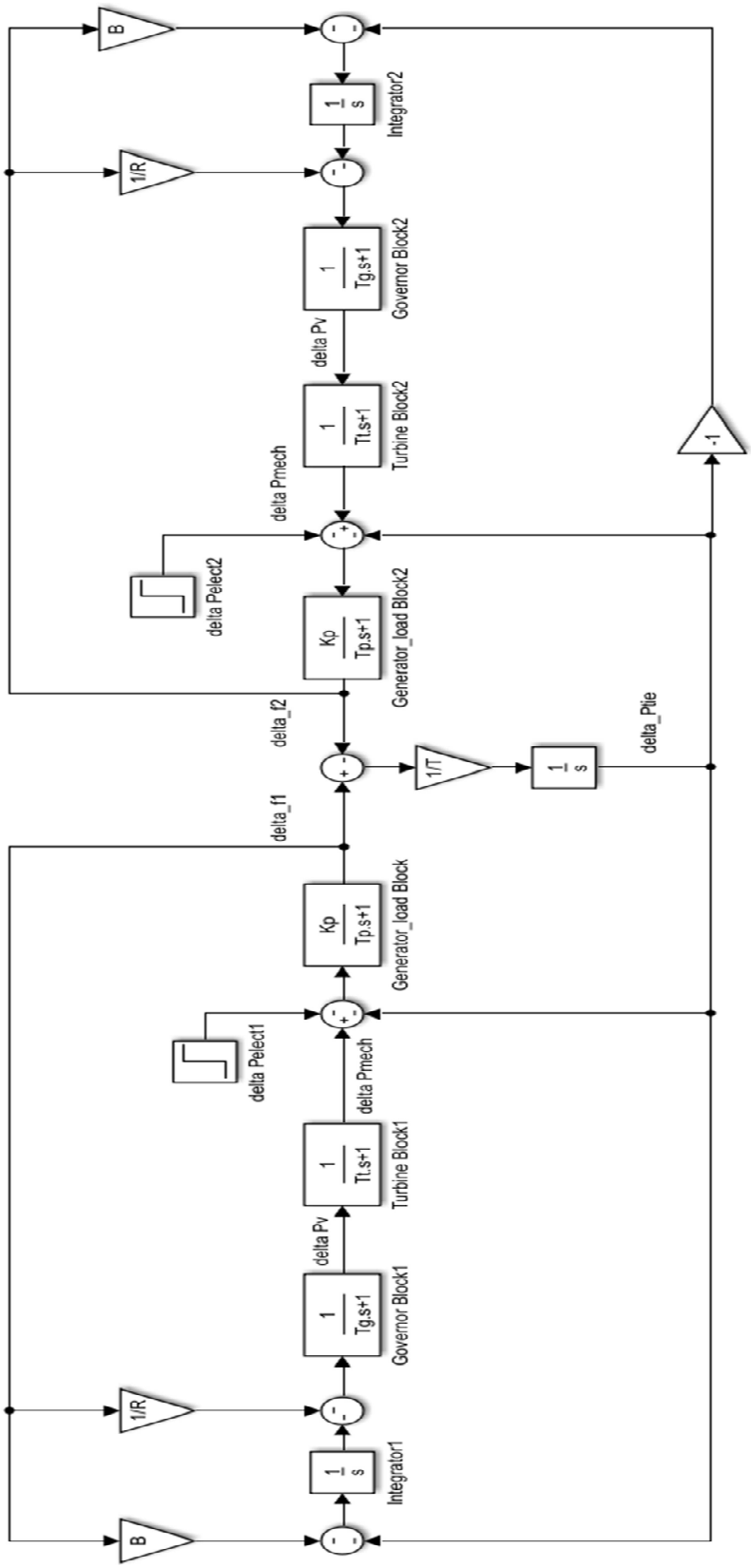

Figure 4.2. Two area load frequency control loop

4.1.2. Delay and False Data Injection attack analysis

In this thesis, we consider the attacks only in the secondary control. The reason for this consideration is that it is difficult for the hijack of the secondary control because of two reasons (i) For most generators which are involved in primary control the measurements are directly taken from the local physical measurements which are barely exposed to attack interference (ii) Even for some generators which send the measurement data through some communication network, have some dedicated communication channels that are very difficult to be attacked even at high costs. On the other hand, the secondary control is built over the communication channel making it vulnerable to attacks. Even the worst attacks against the secondary control have the ability to damage a greater part of the area making the situation riskier. The above figure of the load frequency control is the dynamic model, linearized under small load variance. The dynamic response of the primary and secondary control can be summarized as

4.1.2.1. System Model under Delay attack

Under the delay attack, for convenience, the dynamic variables x(t) can be written as x, and the delayed signal y(t- τ) can be written as y(τ). The dynamics of the frequency control loop under time delay attack are given by (4.19) to (4.22).

$$T_P\dot{\Delta f} = K_P\Delta P_{mech} - K_P\Delta P_{elect} - \Delta f \tag{4.19}$$

$$T_t\dot{\Delta P_{mech}} = \Delta P_V - \Delta P_{mech} \tag{4.20}$$

$$T_g\dot{\Delta P_V} = -\frac{\Delta P_{mech}}{R} - \Delta P_V - \Delta P_C(\tau) \tag{4.21}$$

$$\dot{\Delta Pc} = \beta\Delta f \tag{4.22}$$

Since the time delay attack, TDA is launched against the secondary control, the effect of attack can be modeled as can be $\Delta P_C(\tau)$. (4.23) expresses the above system in matrix form

$$\dot{x} = Ax + A_\tau x(\tau) + Bu \tag{4.23}$$

Where $x(t)$=[Δf ΔP_{mech} ΔP_V ΔP_C] u=[ΔP_{elect}];

$$A=\begin{bmatrix} \frac{-1}{T_p} & \frac{K_p}{T_p} & 0 & 0 \\ 0 & \frac{-1}{T_t} & \frac{1}{T_t} & 0 \\ \frac{-1}{RT_g} & 0 & \frac{-1}{T_g} & 0 \\ \beta & 0 & 0 & 0 \end{bmatrix} \quad A_\tau=\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{-1}{T_g} \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{B}=[-\tfrac{K_P}{T_P}\ 0\ 0\ 0]^{\text{T}}$$

4.1.2.2. System Model under False Data Injection Attack (FDA)

The dynamics of the frequency control loop under false data injection attack are described by (4.24) to (4.27)

$$T_P\dot{\Delta f} = K_P\Delta P_{mech} - K_P\Delta P_{elect} - \Delta f \tag{4.24}$$

$$T_t\dot{\Delta P_{mech}} = \Delta P_V - \Delta P_{mech} \tag{4.25}$$

$$T_g\Delta\dot{P}_V = -\frac{\Delta P_{mech}}{R} - \Delta P_V - (\Delta P_C + \varepsilon\Delta P_C) \tag{4.26}$$

$$\Delta\dot{P}c = \beta\Delta f \tag{4.27}$$

Since the false data injection attack, FDA is launched against the secondary control, the effect of attack can be modeled as can be (ΔP_C+$\in$ $\Delta P_C + K_a$). (4.28) expresses the above system in matrix form as

$$\dot{x} = Ax + Bu \tag{4.28}$$

Where $x(t)$=[Δf ΔP_{mech} ΔP_V ΔP_C] u=[ΔP_{elect}]

$$A=\begin{bmatrix} \frac{-1}{T_p} & \frac{K_p}{T_p} & 0 & 0 \\ 0 & \frac{-1}{T_T} & \frac{1}{T_T} & 0 \\ \frac{-1}{RT_G} & 0 & \frac{-1}{T_G} & 1+\varepsilon \\ \beta & 0 & 0 & 0 \end{bmatrix} \quad B^{T}=\begin{bmatrix} -\frac{Kp}{Tp} & 0 & 0 & 0 \end{bmatrix}$$

4.1.3. Deriving Effective Conditions

Any attack on the system is effective if and only if it can reduce the system performance and destabilize the grid operation. In this section, we drive the effective conditions on the attack parameters that destabilize the power grid. Throughout the thesis, we will consider a simple case when we have only a single area which is under load frequency control

4.1.3.1 TDA analysis:

For any power application, that has a set of dynamic variables set, x $\in R^N$ defined, then there might always exist a minimum time delay 'τ^*' such that for $\tau \geq \tau^*$ the power application becomes unstable. The value of τ^* is called the margin of power application.

Before going further into the derivation of the system we assume that

(i) The original system is stable

(ii) There is no other extra application in the system that can positively interact with the system and reduce the negative impact of TDA

(iii) The change in load power can potentially cause a frequency disturbance in the system.

So, under the following assumptions, the system dynamics are dependent on the system's internal dynamics given by (4.29)

$$\dot{x} = Ax + A_\tau x(\tau) \tag{4.29}$$

So applying Laplace transform and finding the characteristic equation gives us a function of τ that is expressed by (4.30)

$$\Delta(\tau, \lambda) = \det(I\lambda - A - A_\tau) \tag{4.30}$$

$$a(\lambda)+be^{-\lambda\tau}=0 \tag{4.31}$$

$$\text{Where } a(\lambda)= \lambda^4 + a_3\lambda^3 + a_2\lambda^2 + a_1\lambda^1 \tag{4.31a}$$

$$a_3 = T_gT_p + T_gT_t + T_pT_t$$

$$a_2 = T_p + T_g + T_t$$

$$a_1 = 1 + \frac{K_p}{R}$$

$$b = \beta K_p$$

It is known that for a continuous system the roots of characteristic equation (4.31) determine the stability of the system. If the roots lie on the left half of S-plane then the system is said to be stable i.e. the real part of the root needs to be negative, else if the system has any root that lies on the imaginary axis i.e. the real part of the roots are 0, then the system is marginally stable, else if the system has roots whose real parts are positive then the system is unstable.

Let the roots of (4.31) be $\lambda=\sigma + j\omega$, where σ, $\omega \in R$. The time delay attack is effective if and only if the delay τ can keep the roots of (4.31) in RHP (Right Hand Plane). Because (4.31) is quasipolynomial continuous on τ and the initial system is stable and increasing delay should move the roots of (4.31) from LHP (Left Hand Plane) to RHP. Therefore, TDA can be mathematically explained as an input that moves the roots across the imaginary axis with positive speeds. This condition can be expressed by (4.31b)

$$\Delta(j\omega_s, \tau) = 0$$

$$sgn\left(Re\left\{\frac{d\lambda}{d\tau}\right\}\right) > 0 \text{ at } \lambda = j\omega_s \tag{4.31b}$$

Where ω_s is the critical frequency and $\lambda = j\omega_s$ is the critical root of (4.31). Because the roots always exist in pairs for every $\omega_s > 0$ there is a corresponding negative counterpart $-\omega_s$. Therefore, the TDA effective conditions can be expressed as below (4.33) & (4.34)

Here, as we aim at finding a value of τ^* that brings the system to marginal stability we can assume that the real part of the roots is zero and proceed with the calculations. Therefore, in order to find τ first the critical frequency of the system needs to be calculated and then the value of delay. These can be calculated from (4.32)

$$\frac{-b}{a(jw_s)} = e^{jw_s\tau} \tag{4.32}$$

Now if there exists a real critical frequency then term $e^{jw_s\tau}$ can be eliminated and (4.32) can be expressed by (4.33) and (4.34)

$$abs\left(\frac{-b}{a(jw_s)}\right) = 1 \tag{4.33}$$

$$\text{and } w_s\tau = arg\left(\frac{-b}{a(jw_s)}\right) + 2k\pi \quad k \in N^+ \tag{4.34}$$

From 4.33 it can be found that the critical frequency is independent of τ. Given the original system is stable, for any $w_s \in R^+$a delay τ can be found that moves the critical pair of roots from LHP to RHP. If there is no real and positive w_s, then the system is always stable.

If for a single area system, the LFC is not secure naturally, then the TDA margin can be calculated by solving the optimization problem as below

Min τ

Subjected to (4.31b, 4.33, 4.34)

This theory shows that the concept of [13], which says that any time delay τ >0, destabilizes the power system is inaccurate.

The optimization problem shows that the effectiveness of TDA depends on the structure of victim application and TDA strategies, which determine the matrices A, A_τin (4.31). Hence the results in previous work that TDA's effectiveness depends on the grid operating status and that any delay >0 can destabilize the system has proved to be inaccurate.

4.1.3.2. FDA analysis

The assumptions taken for the above single area holds good under this phenomenon also. Here, the characteristic equation is developed from section 4.2.2. takes the form as

$$a(\lambda) = \lambda^4 + a_3\lambda^3 + a_2\lambda^2 + a_1\lambda^1 + b(1+\varepsilon) = 0 \quad (4.35)$$

Because the initial system is stable, the roots of the characteristic equation lie on the left half of the S-plane. The attack parameter ε tries to move the roots lying on the left half of S plane onto the right. Now, finding the critical roots by substituting $\lambda = j\omega$, making real part to zero and finding out the value of ω for the system to be in marginal stability gives us the condition on the proportional constant parameter 'ε'.

The equation after substitution takes the form as

$$(j\omega)^4 + a_3\lambda(j\omega)^3 + a_2\lambda(j\omega)^2 + a_1(j\omega)^1 + b(1+\varepsilon) = 0 \quad (4.36)$$

$$\omega^4 - a_3 j\omega^3 - a_2\omega^2 + a_1 j\omega^1 + b(1+\varepsilon) = 0 \quad (4.37)$$

Making the real and imaginary parts of the above equation (4.37) to zero and by applying Routh-Hurwitz stability criteria for (4.35) we obtain a condition for ε, that keep the system in stable condition. Solving (4.37) gives

$$j(-a_3\omega^3 + a_1\omega^1) = 0 \; ; \quad \omega^4 - a_2\omega^2 + b(1+\varepsilon) = 0$$

Solving above two equations gives $\omega^2 = \frac{a_1}{a_3}$ and $\varepsilon = 1 + \frac{a_1^2 - a_1 a_2 a_3}{b a_3^2}$

Applying Routh Criteria to (4.35) tells that the system is stable if $\varepsilon > -1$. Combining all the conditions together, the system is stable if the value of $\varepsilon \in$ (-1, $1 + \frac{a_1^2 - a_1 a_2 a_3}{b a_3^2}$) elsewhere is unstable.

4.2. Voltage Control Loop

As frequency and voltage are the two parameters that decide the quality of power being delivered to the customers, each parameter is associated with their own control loops. Since we have already studied about the loop associated with the frequency, our next step is to study about the second parameter i.e. voltage control loop.

Though the terminal voltage of the generator is not the exact voltage that is seen at the end user, the user voltage is proportional to the generator terminal voltage. Because the voltage at the end user should be maintained at a certain level the terminal voltage of the generator should also be maintained at its specifications. The terminal voltage of a synchronous generator is governed by the current that is flowing in its field winding. An exciter delivers the DC power to the field winding of a synchronous generator. Explicitly, the excitation system governs the terminal voltage of the generator. There have been a lot of changes in the excitation system that took place over time, technology and ideas. For older generators the excitation system had a DC generator driven by its rotor and power is transferred to the field windings through the slip rings and brushes. Newer generators are excited with static or brushless excitation systems. For the static excitation system, the AC power from the synchronous generator or power from other auxiliary service station is taken and is converted into DC with the help of thyristors and is transferred to the rotor of the synchronous generator with the help of slip rings. For a brushless excitation system, the field and the armature windings are inverted i.e. the rotor had the armature windings and the stator has the field winding. Therefore, the DC power from the thyristor can be directly connected to the field windings without any slip rings.

There were a number of block diagrams developed for modeling this system, one among all that forms the basic block for all the excitation systems known as IEEE type1 exciter is as shown in the Fig. 4.3

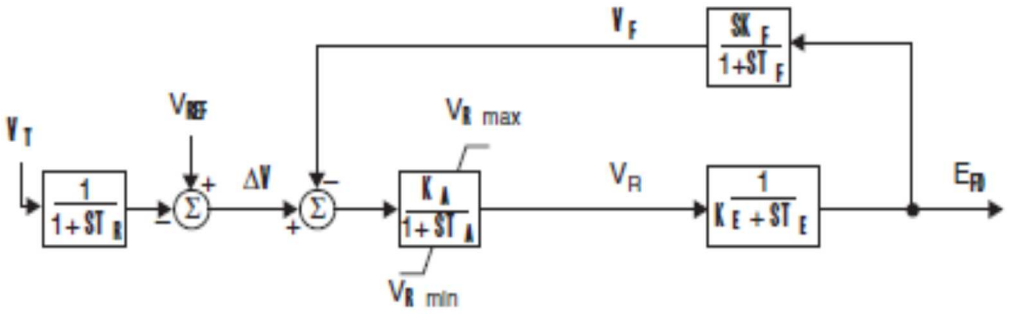

Figure 4.3. IEEE Type1 Excitation System [18]

This block diagram gives the field voltage as the output which is the output of an excitation system, but we are interested in the terminal voltage of the generator so, the output of this block needs to be given a generator block to observe its terminal voltage. When this is done the resultant block diagram can be given by Fig 4.4

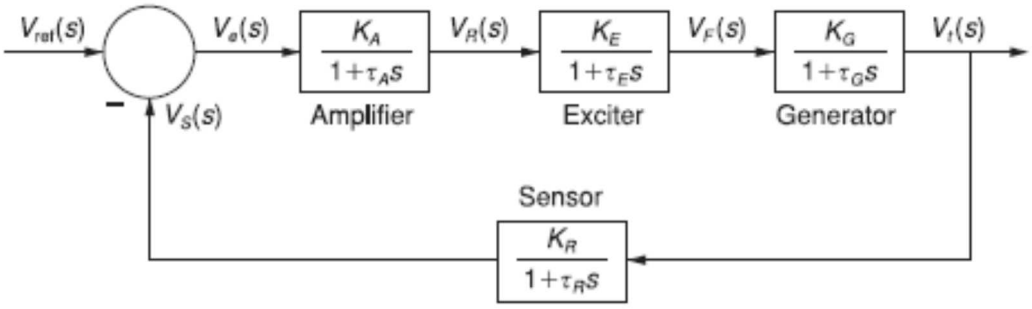

Figure 4.4. Excitation system including generator block

The major components of the voltage control, as can be seen, are amplifier, exciter, generator and sensor/ feedback.

4.2.1. Mathematical Modelling of the components of the Voltage Control Loop

4.2.1.1. Amplifier:

The voltage regulator is modeled as the amplifier. For the simplicity in the analysis, the amplifier is chosen as the first order model. Therefore, its transfer function is given by (4.38)

$$V_r = \frac{1}{1 + ST_a} V_e \tag{4.38}$$

4.2.1.2. Exciter:

As exciter is that part which relates the field voltage of the synchronous generator and the regulator voltage i.e. input to the exciter, a relation between the two voltages is given by the same relation as between the field and the terminal voltage of the generator. The dynamic equation describing the exciter is given by (4.39)

$$\frac{dV_R}{dt} = \frac{1}{T_d}\left(-V_R \ + V_f\right) \tag{4.39}$$

Among the different available excitation systems, brushless DC excitation system shown in Fig.4.5 has been chosen for the analysis as it is neither too old or too new to the industry

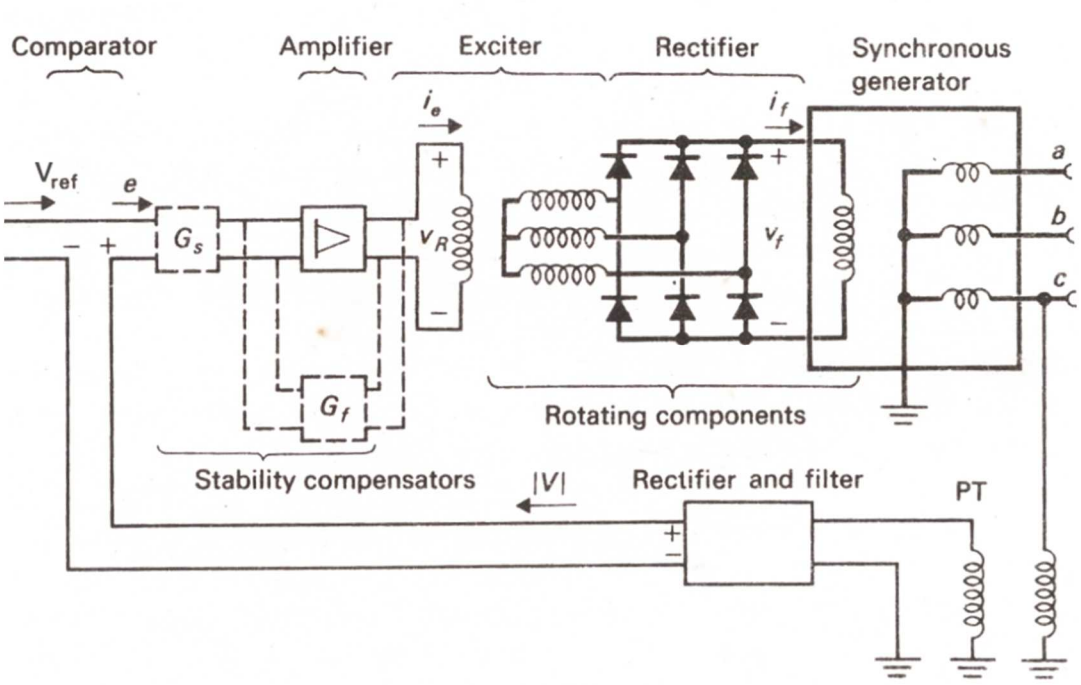

Figure 4.5. Brushless DC excitation system

Source: http://www.srmuniv.ac.in/sites/default/files/files/Chapter3Voltagecontrol.pdf

4.2.1.3. Generator:

Because the exciter input is given to the field windings of the generator a relation between the terminal voltage and field voltage can be used to model the generator block, shown in (4.40)

$$\frac{dV_t}{dt} = \frac{1}{T_d}\left(-V_t \ + V_f\right) \tag{4.40}$$

The Laplace transformed system is given by (4.41)

$$V_t \ = \frac{V_f}{1 + ST} \tag{4.41}$$

4.2.1.4. Sensor:

A potential transformer and a DC rectifier are used as the sensor for the generator terminal voltage. This block is used to improve the dynamics of the exciter and reduce the excessive overshoot.

For any transient stability studies, the initial values of the state variables need to be determined this is obtained by taking that the system is initially operating in the steady state. Combining all the blocks together gives the block diagram of the voltage control loop shown in Fig 4.6

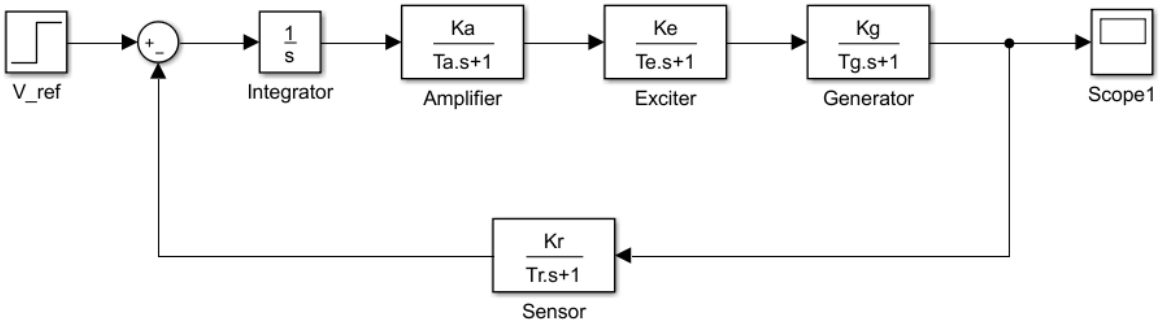

Figure 4.6. Simulation block diagram for voltage control loop

4.2.2. Delay and False Data Injection attack analysis

In this thesis, the attack is considered to occur in the feedback signal as that is the signal which travels back to the control center from the generator output terminal or bus. It has also been assumed that the output voltage of the system is maintained at the reference level until there is a disturbance

in the system load. Because the system voltage depends on the load of the system and any change in the system load can change the voltage of the system, to simulate if the system gets back to its reference voltage after any disturbance a step signal has been given to the reference voltage to accommodate the change in load.

4.2.2.1. System Model under Delay Attack

The dynamics of the system under the time delay attack are given by (4.42)

$$\begin{aligned}
\dot{V}_t &= \left(\frac{K_g}{T_g}\right)V_f - \left(\frac{1}{T_g}\right)V_t \\
\dot{V}_f &= \left(\frac{K_e}{T_e}\right)V_r - \left(\frac{1}{T_e}\right)V_f \\
\dot{V}_r &= \left(\frac{K_a}{T_a}\right)V_a - \left(\frac{1}{T_a}\right)V_r \\
\dot{V}_a &= V_{ref} - V_s(\tau) \\
\dot{V}_s &= \left(\frac{K_r}{T_r}\right)V_t - \left(\frac{1}{T_r}\right)V_s
\end{aligned} \tag{4.42}$$

For our convenience, the dynamic variables x(t) can be written as x, and the delayed signal y(t- τ) can be written as y(τ). Here the time delay attack has been assumed to occur in the feedback or sensor signal therefore the signal V_s has been delayed with a time of τ sec, represented by $V_s(\tau)$. The above set of dynamic equations (4.42) can be written in a matrix form as shown in (4.43)

$$\dot{x} = Ax + A_\tau x(\tau) + Bu \tag{4.43}$$

Where $x=[V_t\ V_f\ V_r\ V_a\ V_s]^T$ $u= V_{ref}$

$$A=\begin{bmatrix} -\frac{1}{Tg} & \frac{Kg}{Tg} & 0 & 0 & 0 \\ 0 & -\frac{1}{Te} & \frac{Ke}{Te} & 0 & 0 \\ 0 & 0 & -\frac{1}{Ta} & \frac{Ka}{Ta} & 0 \\ 0 & 0 & 0 & 0 & 0 \\ \frac{Kr}{Tr} & 0 & 0 & 0 & -\frac{1}{Tr} \end{bmatrix} \quad A_\tau=\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad B=\begin{bmatrix} 0 & 0 & 0 & 1 & 0 \end{bmatrix}^T$$

4.2.2.2. System Model under False Data Injection Attack

If there is a false data injection attack on the feedback signal, then the system dynamic equations are given by (4.44)

$$\begin{aligned} \dot{V}_t &= \left(\frac{K_g}{T_g}\right)V_f - \left(\frac{1}{T_g}\right)V_t \\ \dot{V}_f &= \left(\frac{K_e}{T_e}\right)V_r - \left(\frac{1}{T_e}\right)V_f \\ \dot{V}_r &= \left(\frac{K_a}{T_a}\right)V_a - \left(\frac{1}{T_a}\right)V_r \\ \dot{V}_a &= V_{ref} - V_s(1+\varepsilon) \\ \dot{V}_s &= \left(\frac{K_r}{T_r}\right)V_t - \left(\frac{1}{T_r}\right)V_s \end{aligned} \qquad (4.44)$$

Because the attack is on the feedback signal, V_s has been manipulated to $V_s(1+\varepsilon)$ where ε is the FDI proportional constant. So the system stability depends on the value of ε. So, if the value of ε lies within some limits the system would be stable else the system would be unstable. The motto now is to find out what is that limit of ε when the system is stable.

Because the above equations are linear time dependent equations, (4.44) can be represented in matrix form (4.45)

$$\dot{x} = Ax + Bu \tag{4.45}$$

Where $A=\begin{bmatrix} -\frac{1}{Tg} & \frac{Kg}{Tg} & 0 & 0 & 0 \\ 0 & -\frac{1}{Te} & \frac{Ke}{Te} & 0 & 0 \\ 0 & 0 & -\frac{1}{Ta} & \frac{Ka}{Ta} & 0 \\ 0 & 0 & 0 & 0 & -(1+\varepsilon) \\ \frac{Kr}{Tr} & 0 & 0 & 0 & -\frac{1}{Tr} \end{bmatrix}$ $B=\begin{bmatrix} 0 & 0 & 0 & 1 & 0 \end{bmatrix}^{T}$

and $x=[V_t\ V_f\ V_r\ V_a\ V_s]^{T}$ $u= V_{ref}$

4.2.3. Deriving Effective Conditions

Any attack on the system is effective if and only if it can reduce the system performance and destabilize the grid operation. In this section, we drive the effective conditions on the attack parameters that destabilize the power grid. In this section, effective conditions on different parameters for which the system is stable are derived through analysis and simulations.

4.2.3.1. TDA Analysis

For any power application, that has a set of dynamic variables set, x $\in R^N$ defined, then there might always exist a minimum time delay 'τ^*' such that for $\tau \geq \tau^*$ the power application becomes unstable. The value of τ^* is called the margin of power application.

Before going further into the derivation of the system we assume that

(i) The original system is stable

(ii) There is no other extra application in the system that can support and reduce the negative impact of TDA

(iii) The change in load power can potentially cause a voltage disturbance represented with the help of V_{ref} in the system.

So, under the following assumptions, the system dynamics are dependent on the system's internal dynamics, given by (4.46)

$$\dot{x} = Ax + A_\tau x(\tau) \tag{4.46}$$

So applying Laplace transform and finding the characteristic equation gives us a function of τ that can be expressed as (4.47)

$$\Delta(\tau, \lambda) = \det(I\lambda - A - A_\tau) \tag{4.47}$$

The determinant for the above equation takes the form as a(λ)+b$e^{-\lambda\tau}$=0 where a(λ) is a polynomial in λ and τ is the delay time for the system.

It is known that for a continuous system the roots of characteristic equation tell whether the system is stable or unstable. If the roots lie on the left half of S-plane then the system is said to be stable i.e. the real part of the root needs to be negative, else if the system has any root that lies on the imaginary axis i.e. the real part of the roots are 0, then the system is said to be marginally stable, else if the system has roots whose real parts are positive roots then the system is definitely unstable.

Therefore, TDA can be mathematically explained as an input that moves the roots across the imaginary axis with positive speeds. This condition can be expressed as (4.47a)

$$\Delta(j\omega_s, \tau) = 0$$

$$sgn\left(Re\left\{\frac{d\lambda}{d\tau}\right\}\right) > 0 \quad at\ \lambda = j\omega_s \tag{4.47a}$$

Where ω_s is the critical frequency and $\lambda = j\omega_s$ is the critical root of (4.47). Because the roots always exist in pairs for every $\omega_s > 0$ there is a corresponding negative counterpart $-\omega_s$. Here, as we aim at finding a value of τ^* that brings the system to marginal stability we can assume that the

real part of the roots is zero and proceed with the calculations. Therefore, in order to find τ first the critical frequency of the system needs to be calculated and then the value of delay. These can be calculated from (4.48)

$$\frac{-b}{a(jw_s)} = e^{jw_s\tau} \tag{4.48}$$

Now if there exists a real critical frequency then term $e^{jw_s\tau}$ can be eliminated and (4.48) can be expressed by (4.48a), (4.48b)

$$abs\left(\frac{-b}{a(jw_s)}\right) = 1 \tag{4.48a}$$

$$\text{and } w_s\tau = arg\left(\frac{-b}{a(jw_s)}\right) + 2k\pi \tag{4.48b}$$

From (4.48a) it can be found that the critical frequency is independent of τ. Given the original system is stable, for any w_s a delay τ can be found that moves the critical pair of roots from LHP to RHP. If there is no $w_s$which is real and positive then the system is said to be always stable.

If for a single area system, the LFC is not secure naturally, then the TDA margin can be calculated by solving the below optimization problem.

Min τ

Subjected to (4.47a, 4.48a, 4.48b)

This theory shows that the concept of [13], which says that any time delay τ >0, destabilizes the power system is inaccurate.

4.1.3.2. FDA analysis

The assumptions for the single area taken above holds good under this phenomenon also. So here also we need to develop the characteristic equation from the equations in 4.46.

It takes the form as $a(\lambda) = \lambda^4 + a_3\lambda^3 + a_2\lambda^2 + a_1\lambda^1 + b(1+\varepsilon) = 0$ (4.49)

Because the initial system is stable the roots of the characteristic equation lie on the left half of the S-plane. And because there is an attack the parameter ε tries to move the roots lying on the left half of S plane onto the right. Now, finding the critical roots by substituting $\lambda = j\omega$, making real part to zero and finding out the value of ω for the system to be in marginally stable condition gives us the condition on the proportional constant parameter 'ε'.

(4.49) after substitution of the value of λ takes the form (4.50)

$$(j\omega)^4 + a_3\lambda(j\omega)^3 + a_2\lambda(j\omega)^2 + a_1(j\omega)^1 + b(1+\varepsilon) = 0 \quad (4.50)$$

$$\omega^4 - a_3 j\omega^3 - a_2\omega^2 + a_1 j\omega^1 + b(1+\varepsilon) = 0 \quad (4.51)$$

Making the real and imaginary parts of the above equation (4.51) to zero and by applying Routh-Hurwitz stability criteria for (4.49) we obtain a condition for ε, that keep the system in stable condition. Solving (4.51) gives

$$j(-a_3\omega^3 + a_1\omega^1) = 0 \quad ; \quad \omega^4 - a_2\omega^2 + b(1+\varepsilon) = 0$$

Solving above two equations gives $\omega^2 = \frac{a_1}{a_3}$ and $\varepsilon = 1 + \frac{a_1^2 - a_1 a_2 a_3}{b a_3^2}$ saying that the system is marginally stable at the above value of ε and is stable for values below that value. Applying Routh Criteria to (4.49) tells that the system is stable if $\varepsilon > -1$. Combining all the conditions together, the system is stable if the value of $\varepsilon \in$ (-1, $1 + \frac{a_1^2 - a_1 a_2 a_3}{b a_3^2}$) elsewhere is unstable.

CHAPTER V

EXPERIMENTAL SETUP AND SIMULATION RESULTS

5.1 Experimental Setup for FCL

We demonstrate the above-explained concepts through simulation studies. We used Simulink in order to set up the block diagram and Matlab to calculate the critical values of the cyber-attack parameters. The values for different parameters of an area are taken from [1] shown in Table 5.1. It has been assumed that the areas are identical so the values of all the parameters are assumed same. All the values of parameters and plots are expressed in p.u. Initially, the power grid is stable and a load change is assumed at 10 sec.

Table 5.1. Parameters of single area LFC

T_T	T_G	T_P	K_P	R	B
0.1	0.3	10	1	0.05	12.6

5.2. Results

All the results obtained are for the frequency deviation under different attack scenarios. Under any scenario if the frequency deviation goes to zero i.e. the system gets back to its nominal frequency after some time, then the system under that particular condition is stable, else the system is unstable. For all the cases there is a load change of 0.1 p.u applied at t=10 sec.

5.2.1. Power system with no AGC

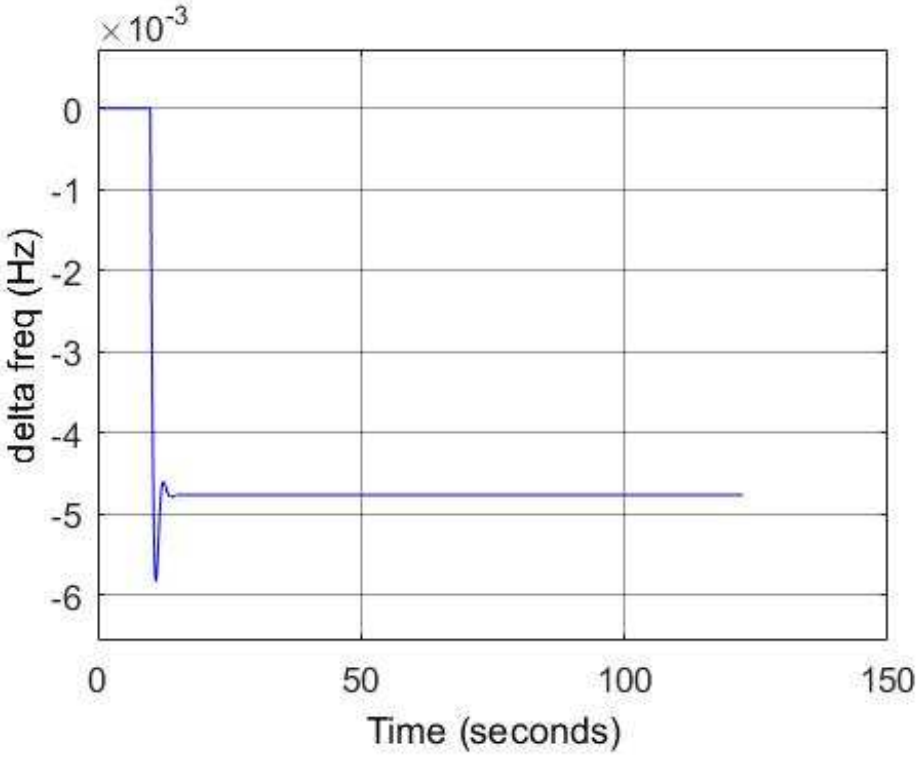

Figure 5.1 Frequency deviation with no AGC control

When the frequency control loop has only governor control with no AGC and the system experiences a change in load at t=10 sec, the frequency of the system gets disturbed for a while and gets stabilized but not at the nominal value after some time seen from Fig.5.1.

5.2.2. System with AGC

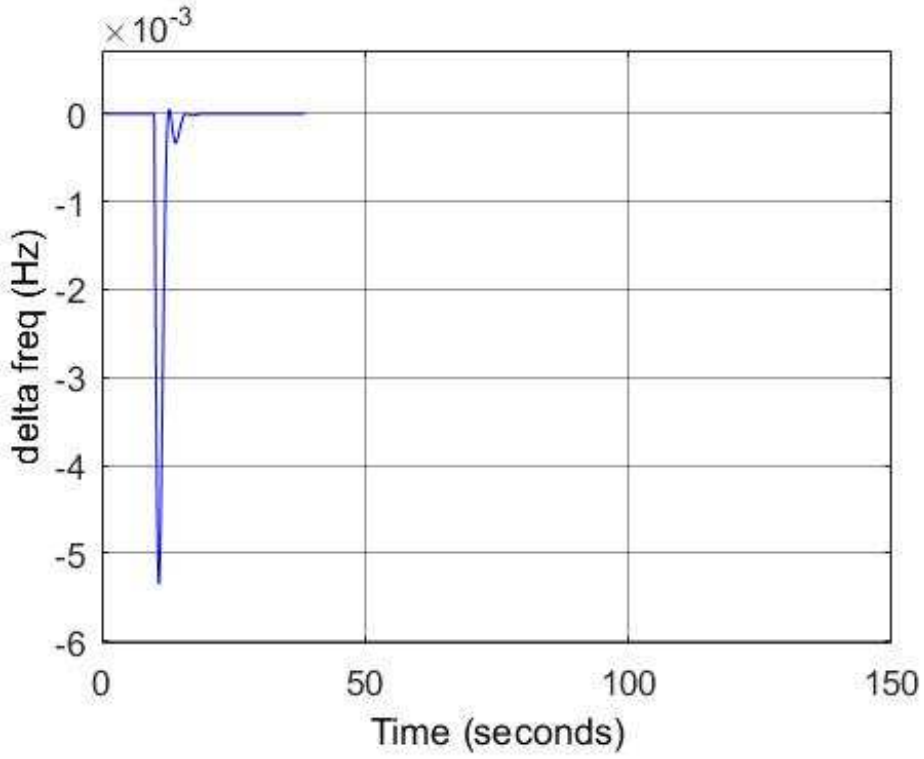

Figure 5.2 frequency deviation with AGC

When the system has AGC control along with the governor control and when there is a disturbance in the system, the frequency initially fluctuates for some time immediately after the disturbance, then gets stabilized at the nominal value seen in Fig.5.2. Here, the change in frequency goes to zero which means that the system is getting back to its nominal value after the disturbance. This is the advantage of using system with AGC block.

5.2.3. System under time Delay attack with τ=1 sec

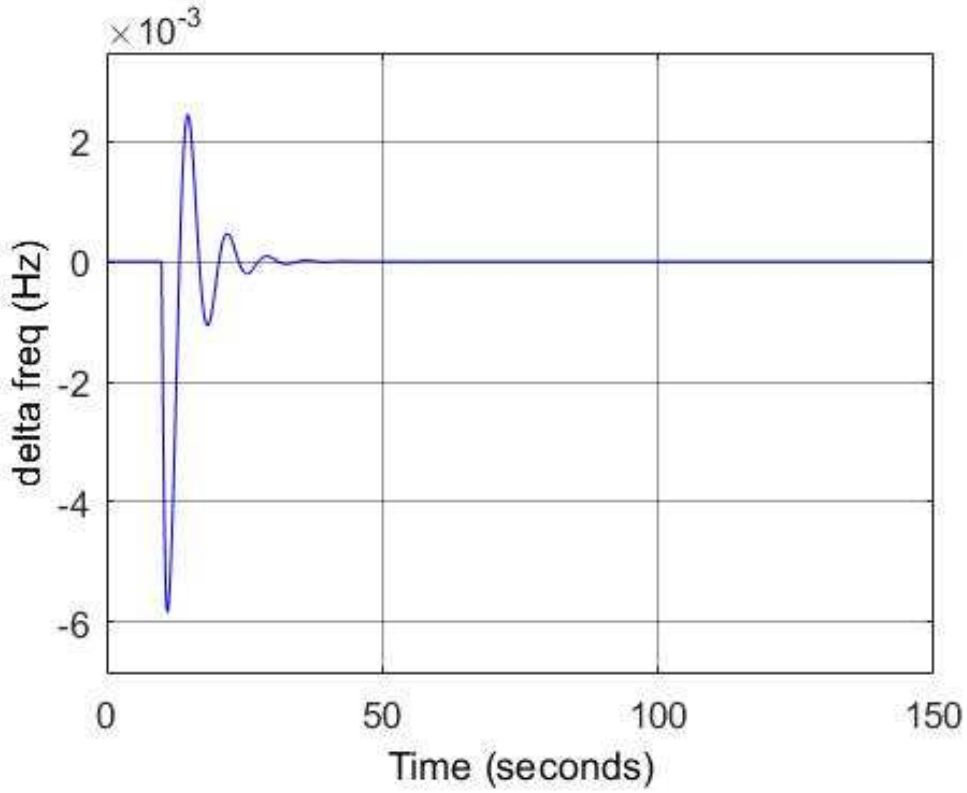

Figure 5.3 frequency deviation with delay τ=1 sec

When there is a delay of 1 second introduced for the signal going from the AGC center to the Governor and there is load change in the system at t=10 sec, the frequency of the system fluctuates for a while and then settles down at the nominal value in the steady state. Meaning, even though there is a delay introduced in the system it still operates in the stable region seen from the Fig.5.3

5.2.4. System with Delay τ=2.047 sec

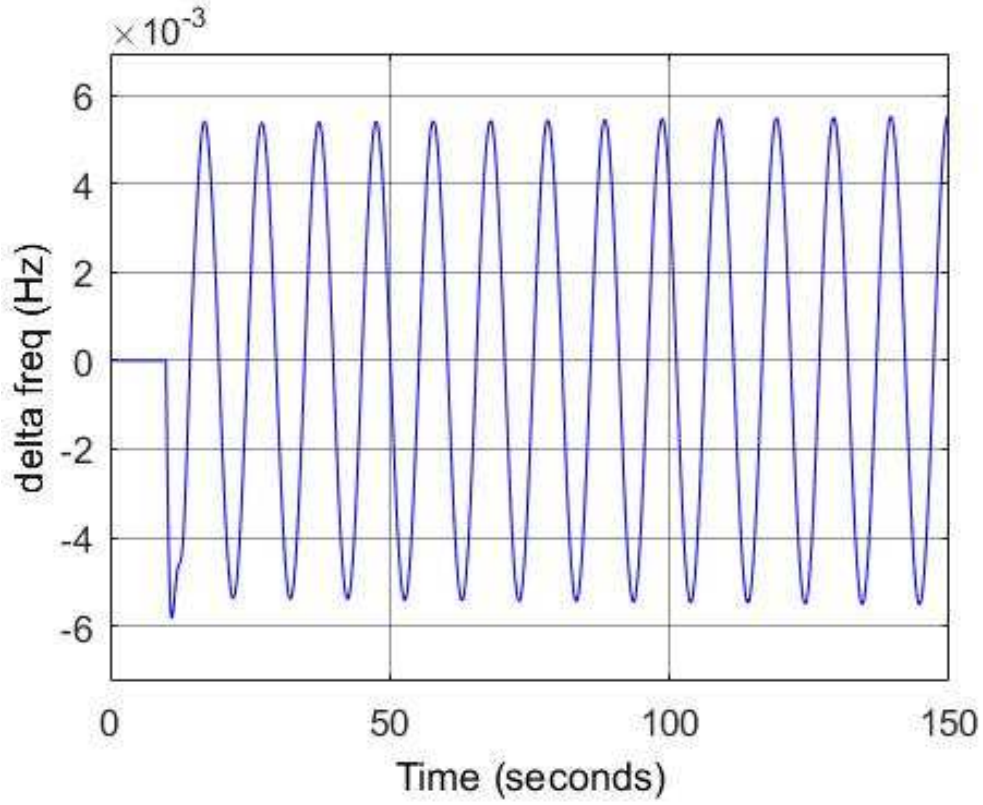

Figure 5.4 frequency deviation with delay τ=2.047 sec

When the delay in the system is increased to t=2.047 seconds, and load changes by 0.1 p.u at t=10sec, then the frequency deviation of the system keeps on oscillating and do not come to a stable position i.e. the system is in marginally stable condition. This can be seen from the Fig.5.4. The optimal conditions for which the system remains in stable region are obtained by solving the optimization problem described in Section 4.1.3.1.

5.2.5. System with Delay τ=2.1sec

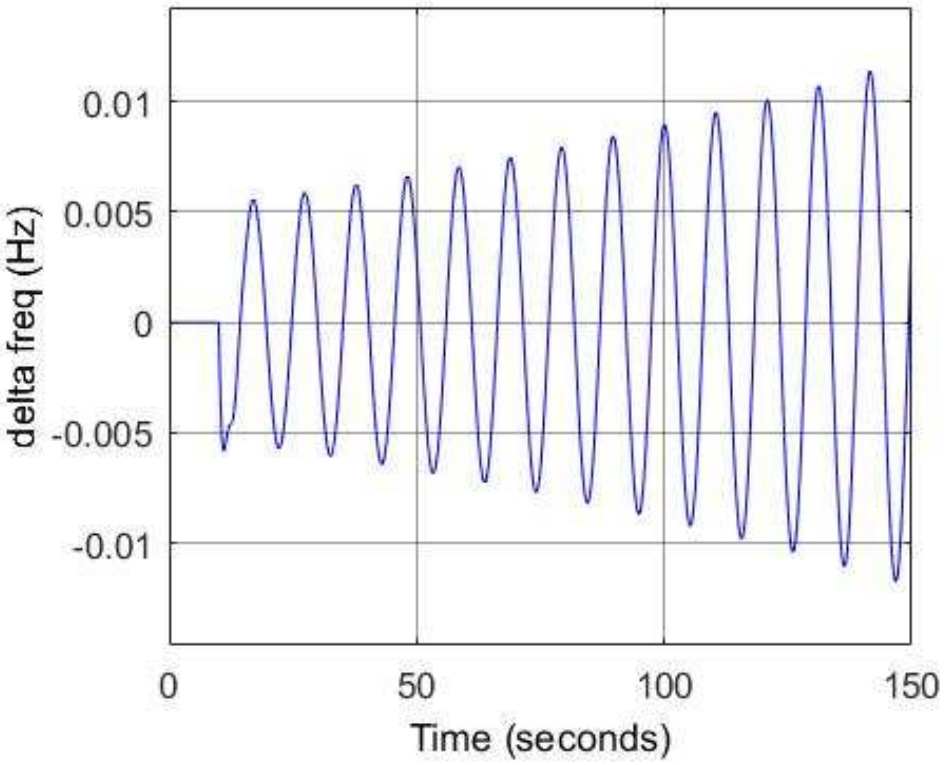

Figure 5.5 frequency deviation with delay τ=2.1 sec

When a delay in the system is t=2.1 seconds which is greater than the delay for the marginally stable condition, naturally the system moves into the unstable condition and the frequency deviation always keeps on increasing. This can be seen from the Fig.5.5.

Therefore, it is clear from the above results that the system remains stable for some delay but becomes unstable for larger values. Therefore, by keeping the value of delay within the determined range the system can be operated in the stable region despite of a cyber-attack.

5.2.6. System with False Data Injection Attack with ε =2 and bias=1

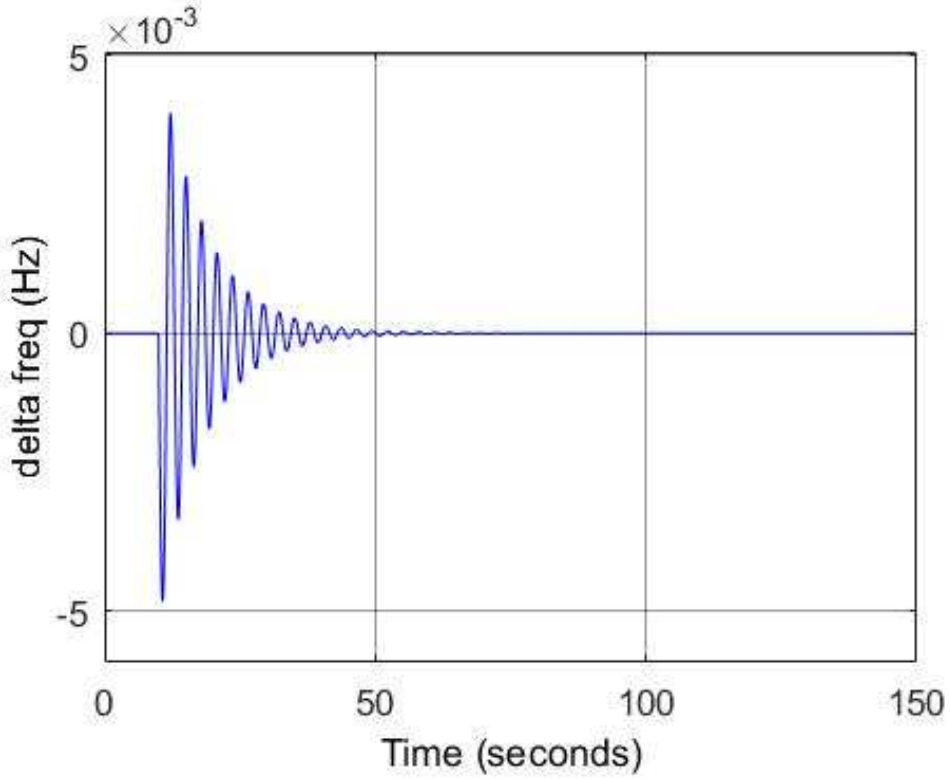

Figure 5.6 frequency deviation with ε =2 and bias=1

When the system is attacked with the false data injection attack with the proportional attack constant ε =2 and the bias constant=1, and load change of 0.1 p.u at t=10 sec, then the system goes to stable condition after some time. This can be seen from Fig. 5.6

5.2.7. System with False Data Injection Attack with ε =2.55 and bias=1

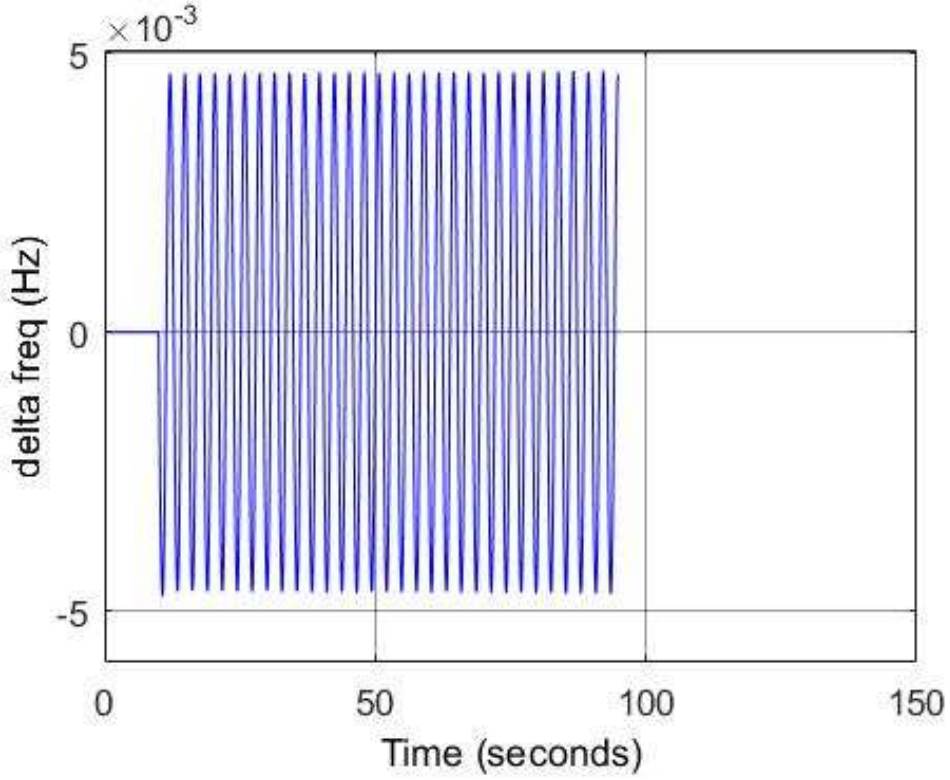

Figure 5.7 frequency deviation with ε =2.55 and bias=1

When the system is attacked with the false data injection attack with the proportional attack constant ε =2.55 and the bias constant=1, and load change of 0.1 p.u at t=10 sec, then the system goes to marginal stable condition and the system frequency keeps oscillating seen from Fig. 5.7.

The conditions for the marginal stability can be found by solving the characteristic equation of the system.

5.2.8. System with False Data Injection Attack with ε =3 and bias=1

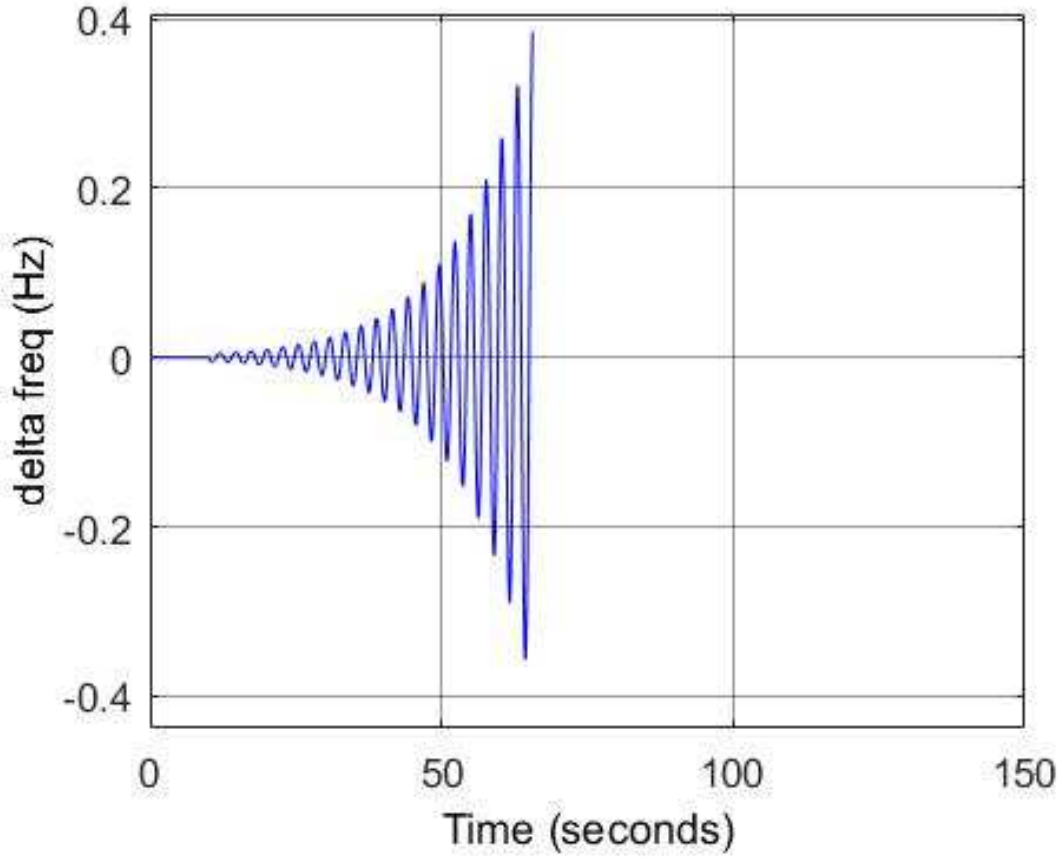

Figure 5.8. frequency deviation with ε =3 and bias=1

Fig. 5.8 shows that when the system is attacked with the false data injection attack having proportional attack constant ε =3, bias constant=1, and load change of 0.1 p.u at t=10 sec, since the value of ε is greater than the marginal stable condition values obtained from the analysis in Section 4.1.3.2, the system goes to unstable condition and the system frequency oscillations keeps on increasing.

5.2.9. System with delay=1 sec and FDA with ε =1 and bias=1

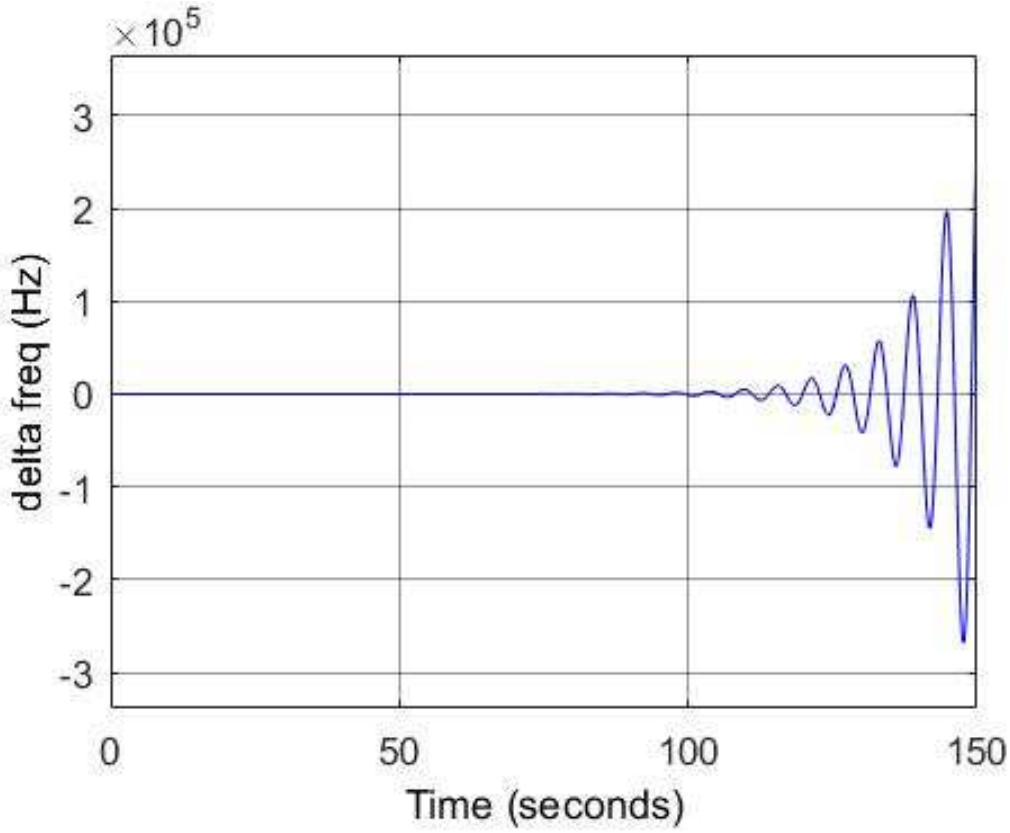

Figure 5.9 frequency deviation with delay=1sec, ε =3 and bias=1

The system when subjected to a deterministic delay of 1 sec and a false data injection error with ε =0.5 and bias=1, it has been observed that the system moves to instability and the frequency of the system does not come to a stable value as shown in Fig. 5.9

The thing to be noted here is that even though the system remains stable when attacked by the same individually when both attacks are acted on the system simultaneously, the system moves to an unstable condition.

5.3. Experimental Setup for VCL

The above-demonstrated concepts are explained through the simulation studies. We used Simulink in order to set up the block diagram and Matlab to calculate the critical values of the cyber-attack parameters. The values for different parameters shown in Table.5.2 are taken from [18]. Values of parameters and the plots are expressed in p.u. Initially, the grid voltage is at its reference value a load change at t=10 sec has caused a change in system voltage. In order to bring it back to the reference value a unit step reference voltage value is given as the input. The values of the parameters for the voltage control loop are given as

Table 5.2. Parameters for the Voltage Control Loop

T_a	K_a	T_e	K_e	T_g	K_g	T_r	K_r
0.1	1	0.4	1	1	1	0.01	1

5.4. Results for VCL

All the results obtained are for the terminal voltage of the generator under different attack scenarios. Analysis has shown that the system under time delay attack is stable if the value of time delay is less than 0.715 sec, that means any delay greater than that makes the system unstable

Similarly, when the system is under the False Data Injection Attack the system is stable if the value of the FDA proportionality constant is in between -1 and 1.55.

Let us now look at the simulation results for the system under different values of the attack parameters.

5.4.1. System under time delay attack with τ=0.5 sec

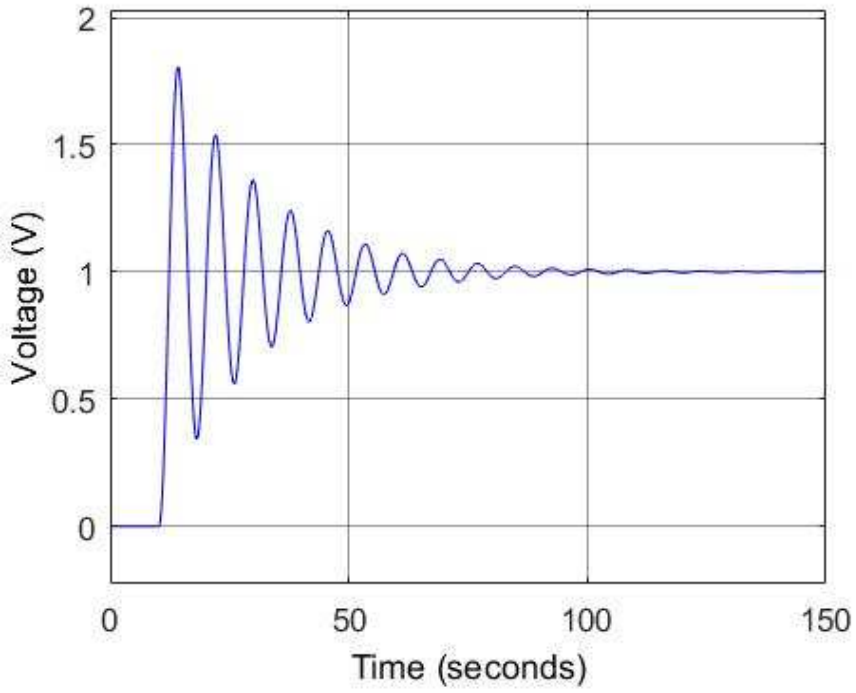

Figure 5.10. System voltage with delay time= 0.5 sec

When the system is subjected to the time delay attack with a delay of 0.5 sec and there is a load change at t=10 sec, the system voltage fluctuated for some time but settled at a constant value as in Fig.5.10. This shows that the system is stable and is operating at the required voltage level even after the attack.

5.4.2. System under delay attack with delay τ=0.715 sec

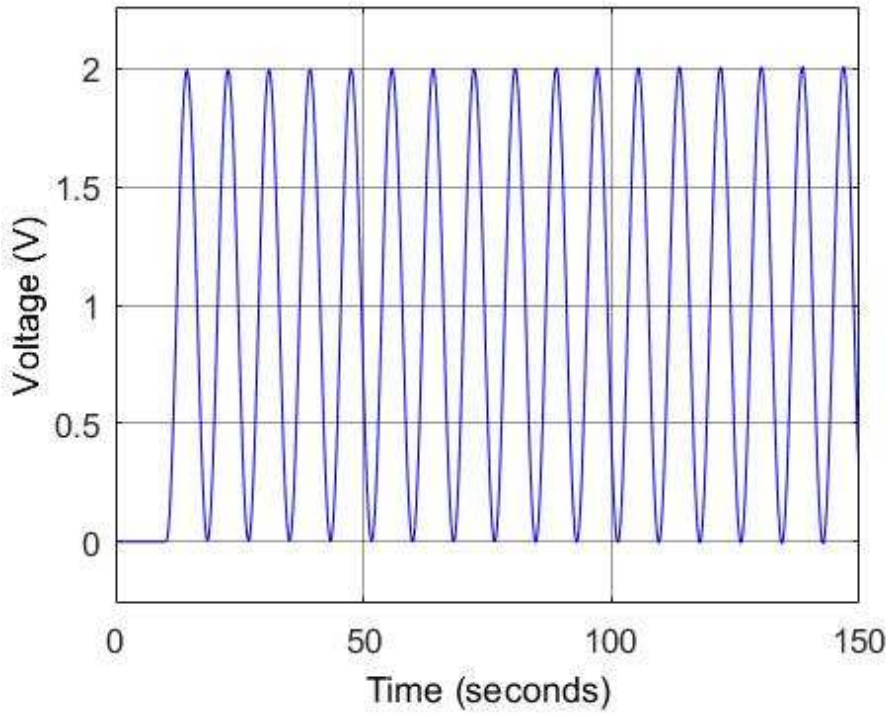

Figure 5.11. System Voltage with delay=0.715 sec

Analysis form Section 4.2.3.1 showed that the system is marginally stable when a delay of is 0.715 seconds is applied to the system. It can be seen in Fig.5.11 that the system voltage is always oscillating with time. As these oscillations are neither increasing nor decreasing with time, the system is said to be in marginal stable condition.

5.4.3. System with Delay= 0.8 sec

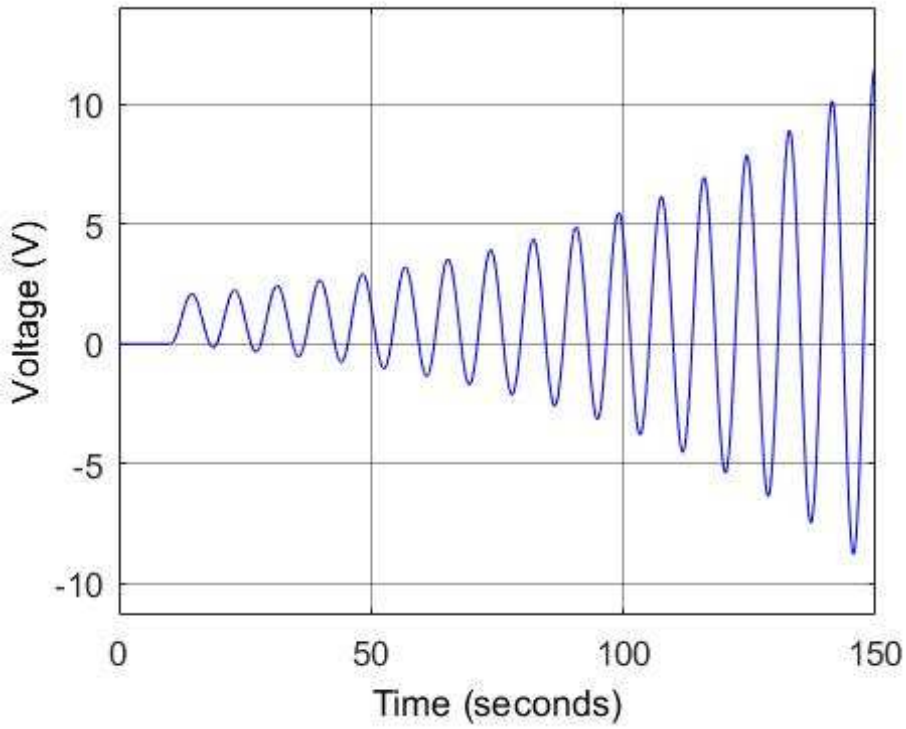

Figure 5.12. System voltage when delay= 0.8 sec

When the delay is 0.8 seconds greater than the marginal value obtained through analysis, the system can be clearly seen to be unstable because the oscillations for the system voltage are always increasing with respect to time shown in Fig. 5.12.

5.4.3. System under false data injection with ε =1

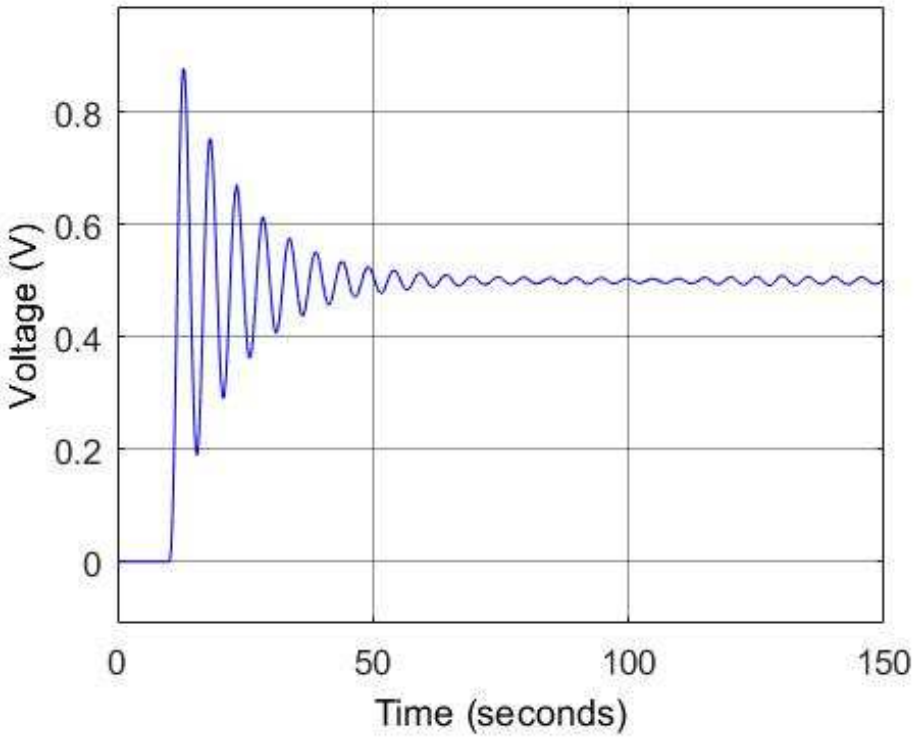

Figure 5.13. System voltage under FDA with ε =1

Under the false data injection, analysis has shown the feasible region is (-1, 1.55). So, when the FDA proportional constant has been taken to be 1, the system voltage oscillates for some time and gets backs to a stable operating value after that, showing that the system is stable as in Fig 5.13.

5.4.4. System under false data injection with ε =1.55

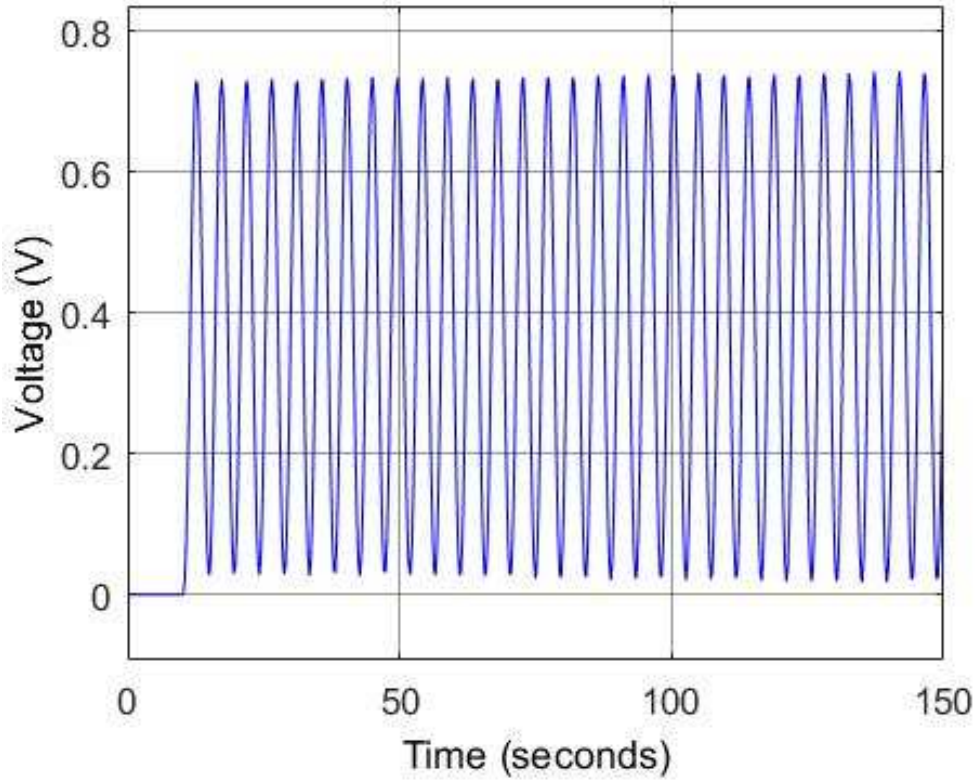

Figure 5.14. System voltage under FDA with ε =1.55

When the value of ε is chosen to be 1.55 the edge point in the region of stability, the system voltage is observed to be completely oscillatory, Fig 5.14. The oscillations of the system do not reduce or increase in their magnitude with respect to time, therefore the system voltage is said to be in marginal stable condition.

5.4.5. System under false data injection with ε =2

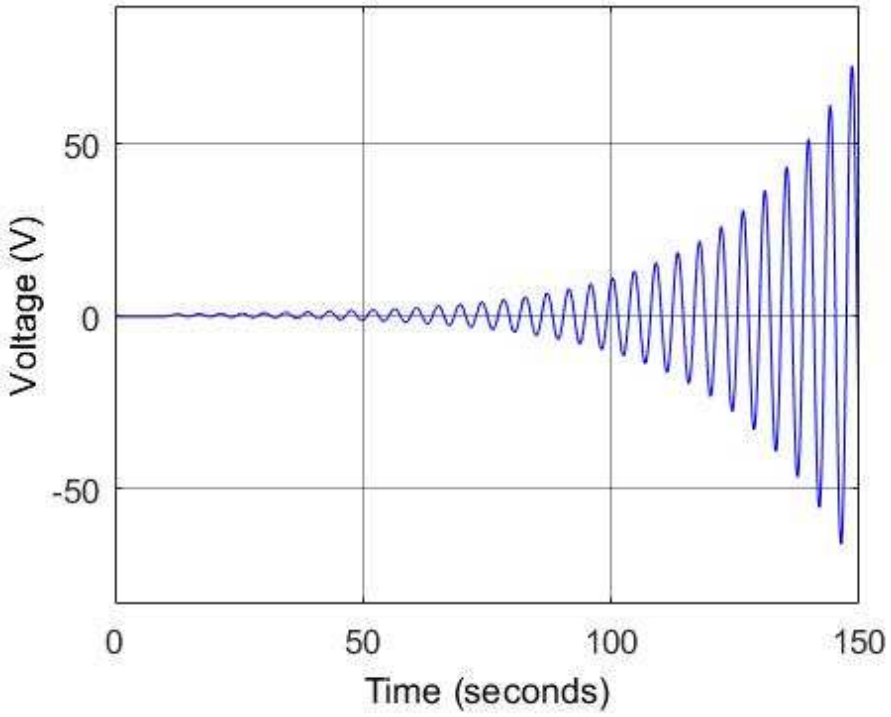

Figure 5.15 System voltage under FDA with ε =2

Because the value of ε is beyond than the set of values obtained from the analysis showing the stability, the voltage oscillations keep on increasing with respect to time shown in Fig. 5.15, making the system to be unstable.

5.4.6. System under both Delay attack and FDA attacks

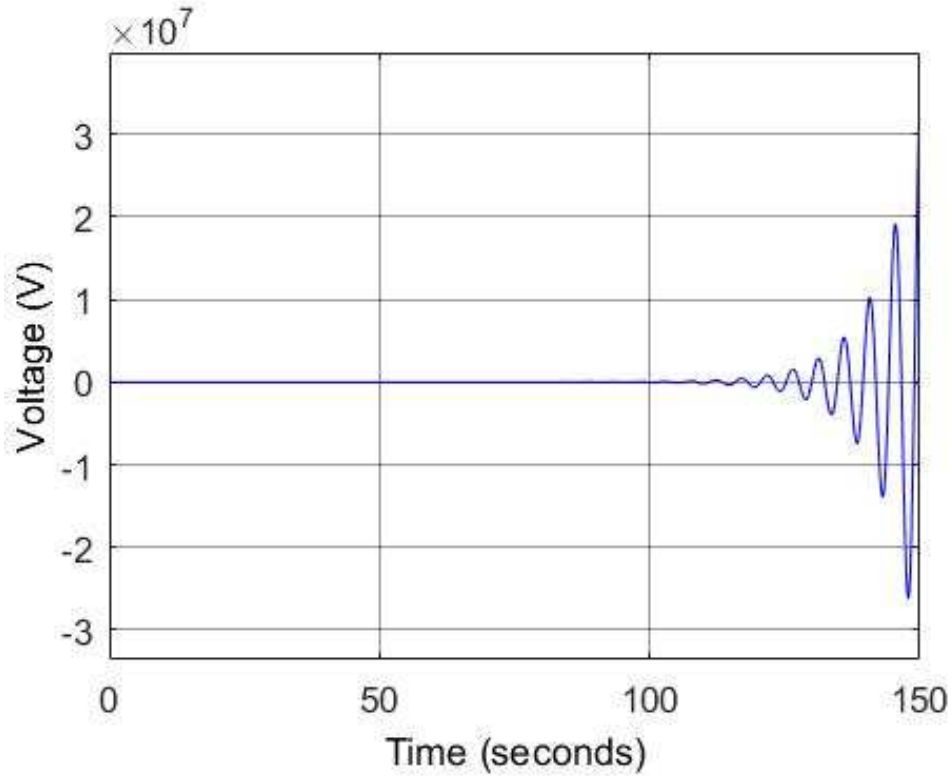

Figure 5.16. System with delay τ =0.5 and ε =1

It can be clearly seen that the system voltage is stable when both the attacks launched separately, but when both of them attack the system at the same time then the system becomes unstable with increasing oscillations with respect to time shown in Fig 5.16.

CHAPTER VI

CONCLUSION AND FUTURE WORK

6.1 Conclusion

In this thesis, we propose an analytical framework deriving the conditions for a simple power system model being attacked with two different cyber attacks. To demonstrate the effect of these attacks two important loops of the power system, frequency control loop and the voltage control loop are taken with specified values for different parameters. The mathematical equations governing different blocks of the control loop are taken and the dynamic model for the control loops have been developed. The equations were inscribed with the attack and the attack model was developed. Finally, a mathematical analysis has been conducted to find out the range of values for the parameters that keep the system in stable operation were developed. The obtained range is verified by simulating the control loops in Simulink with different values of the attack parameters and see if the system is in stable condition or not. Though the proposed methods and optimal conditions obtained for different control loops are demonstrated for a simple case; they can be applied to other forms of control applications also. This work can be considered as the starting step for the analysis of the cyber attacks on the power system loops.

6.2. Future Work

In the thesis, we do not consider any effects on or of the power market, but in reality, they have a huge impact on the fuel and energy prices, operation and performance of the generators in the system over a long time. So, studies on the uncertainty of such factors can be considered in future work.

In the thesis, it has been assumed that the values of the parameters in the system are known but in reality, it is difficult to get the exact values of the equivalent damping constants of the generators and equivalent load models in the system.

Till now we studied the impact of different types of uncertainties but haven't seen any techniques for suppressing the effect of these uncertainties. So future work could be, developing techniques to reduce these uncertainties.

Finally, moving forward, we foresee power system being operated with a tight coupling between cyber and physical components in generation, transmission and distribution systems. There should be a proper understanding of all sorts of uncertainties before any new technology is introduced into the system. This thesis provides some e□orts toward this direction; more work is still needed to ensure the reliability of the system.

REFERENCES

[1] J.K.Wang and Chunyi Peng, (2017) "Analysis of Time Delay Attack against Power Grid Stability". In proc. of *the 2nd workshop on Cyber-Physical Security and Resilience in Smart Grids,* Pittsburgh, PA, USA, April 2017(CPSR-SG'17)

[2] "Vulnerability analysis of energy delivery control systems," Idaho National Laboratory, Sep. 2011 [Online]. Available: http://energy.gov/

[3] S. Wang, X. Meng, and T. Chen, "Wide-area control of power systems through delayed network communication," *IEEE Trans. Control Systems Technology*, vol. 20, no. 2, pp. 495–503, Mar. 2012.

[4] J. Zhang and A. D. Domínguez-García, "On the impact of communication delays on power system automatic generation control performance," in *Proc. North American Power Symposium*, Sep. 2014.

[5] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Automatic Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[6] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Proc. of International Conference on Hybrid Systems: Computation and Control,* 2009.

[7] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla, and S. Sastry, "Foundations of control and estimation over lossy networks," *Proc. IEEE*, vol. 95, no. 1, pp. 163–187, Jan. 2007.

[8] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *Proc. ACM Conference on Computer and Communications Security*, 2009, pp. 21–32.

[9] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," *Proc. of IEEE International Conference on Smart Grid Communications*, Oct. 2010, pp. 226–231.

[10] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system," *Proc. of IEEE Power and Energy Society General Meeting*, Jul. 2010.

[11] J. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems," *Proc. IEEE*, vol. 95, no. 1, pp. 138–162, Jan. 2007.

[12] J. Nilsson, "Real-time control systems with delays," Ph.D. dissertation, Lund Institute of Technology, Lund, Sweden, 1998.

[13] S. Carullo and C. Nwankpa, "Experimental validation of a model for an information-embedded power system," *IEEE Trans. on Power Delivery*, vol. 20, no. 3, pp. 1853–1863, Jul. 2005.

[14] J. Nutaro and V. Protopopescu, "The impact of market clearing time and price signal delay on the stability of electric power markets*," IEEE Trans. on Power Systems*, vol. 24, no. 3, pp. 1337–1345, Aug. 2009.

[15] [online]. http://www.oe.if.ua/showarticle.php?id=3413

[16] [online]. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[17] [online]. http://www.ukrinform.net/rubric-crime/1937899-russian-hackers-plan-energy-subversion-in-ukraine.html

[18] J.D.Glover, M.S.Sarma, T.J.Overbye, "Power System Controls", in *Power System Analysis and Design*, 5th edition, Cengage Learning, 2012, ch.12

VITA

SAI LALITHA DATTATREYA POOSARLA

Master of Science

Thesis: IMPACTS OF TIME DELAY AND FALSE DATA INJECTION ATTACKS ON POWER SYSTEM CONTROL LOOPS

Major Field: Electrical and Computer Engineering

Biographical:

Education:

Completed the requirements for the Master of Science in your major at Oklahoma State University, Stillwater, Oklahoma in July 2017.

Completed the requirements for the Bachelor of Science in Electrical and Electronics Engineering at JNTUK, Kakinada, India in 2015.

Professional Memberships: Honor Society of Phi Kappa Phi