In this work, we study the impacts of Denial-of-Service (DoS) attacks on the cyber-physical implementation of wide-area control. The controller is designed as a Linear Quadratic Regulator (LQR) for damping power flow oscillations. We first derive a nominal mathematical model of the power system network considering a delay-aware LQR controller without any DoS. Thereafter, we model how DoS enters the closed-loop dynamics of this system by considering the Hadamard product of the LQR gain matrix with a matrix of attacked links. We propose two mitigation strategies to compensate for the loss of missing states in the feedback path, and test their effectiveness against three variables of interest - namely, location of attack, time of attack, and duration of attack. We design a decision tree classifier for each strategy based on these parameters to predict the severity of an attack. The results are illustrated with a DoS simulation on the standard IEEE 4-machine Kundur model and 14-machine Australian model.
Mitigation of Denial-of-Service Attacks on Wide-Area Power Systems

by
Nachiappan Chockalingam

A thesis submitted to the Graduate Faculty of
North Carolina State University
in partial fulfillment of the
requirements for the Degree of
Master of Science

Electrical Engineering

Raleigh, North Carolina

2016

APPROVED BY:

__________________________  ____________________________
Dr. Troy Nagle               Dr. David Lubkeman

__________________________
Dr. Aranya Chakrabortty
Chair of Advisory Committee
BIOGRAPHY

The author was born in Chennai, Tamil Nadu, India on the 13th of December 1990. He received a Bachelor’s degree in Instrumentation and Control Engineering from National Institute of Technology, Tiruchirappalli, India in 2012. He was a System Integration Engineer at Caterpillar India Private Limited working on machine controls integration for 2 years before joining NC State University in 2014 for his Master of Science degree in Electrical Engineering. His research interests include optimal control, cyber-physical systems and automotive electronics.
ACKNOWLEDGEMENTS

First and foremost, I would like to thank my adviser Dr. Aranya Chakrabortty for his guidance in my thesis work and his amazing lectures in Control Theory which have inspired me to continue my graduate studies in that area of expertise. His humble attitude and helpful nature made my first steps in academic research a fulfilling and exciting experience. I am lucky to have had the chance to work with Dr. Chakrabortty, who is at the forefront of research using WAMACS technology. He is also one of the best instructors that I have had, he enjoys teaching as well as research and I have learned a lot from his courses.

I would also like to thank Dr. David Lubkeman and Dr. Troy Nagle for being part of my graduate committee. Dr. David Lubkeman is an incredible instructor and has, what seems to be an infinite amount of knowledge, regarding SCADA systems and communications. I attended Dr. Troy Nagle’s Digital Controls course was impressed by his expertise in the field. I have learnt a lot from the interactions I have had with him during the course.

I would also like to thank FREEDM center for providing the space and resources for this research effort. I would like to thank Dr. Chakrabortty’s research team for the inspiration and support they provided.

Finally, I would like to thank my family and friends who have supported me in all my endeavors and encouraged me to pursue graduate studies.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>LIST OF TABLES</th>
<th>vi</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIST OF FIGURES</td>
<td>vii</td>
</tr>
</tbody>
</table>

## Chapter 1 INTRODUCTION
1.1 Wide-Area Measurement and Control ........................................... 3
1.2 Motivation of the Study .............................................................. 4
1.3 Literature Review ........................................................................... 5
1.4 Organization of Thesis ................................................................... 9

## Chapter 2 Wide Area LQR Control ................................................... 11
2.1 Dynamic Model of a Power System ................................................. 11
  2.1.1 Synchronous Generator Models ................................................... 11
  2.1.2 Load Models ............................................................................. 14
  2.1.3 Transmission Line Models .......................................................... 15
  2.1.4 Network Dynamic Models ............................................................ 15
  2.1.5 Small-Signal Model .................................................................. 17
2.2 Power System with Delays ............................................................... 25
  2.2.1 Cyber-Physical System Architecture ............................................ 26
  2.2.2 System with Network delays ......................................................... 29
2.3 LQR Control Design ..................................................................... 31
  2.3.1 Optimizing the state cost Q ......................................................... 32

## Chapter 3 CYBER ATTACKS AND MITIGATION .................................. 35
3.1 Denial-of Service Attacks ............................................................... 37
  3.1.1 Security Attack Parameters .......................................................... 38
  3.1.2 Performance Criteria ................................................................. 39
  3.1.3 Mitigation Strategy ................................................................. 40
3.2 Severity Classification .................................................................. 41

## Chapter 4 SIMULATION AND RESULTS .......................................... 45
4.1 Kundur Power System Model .......................................................... 46
  4.1.1 Small Signal Model ................................................................. 46
  4.1.2 Cyber-physical model ............................................................... 48
  4.1.3 Cyber-Attack Simulation ............................................................ 50
4.2 Australian power system model ...................................................... 60
  4.2.1 Small Signal Model ................................................................. 61
  4.2.2 Cyber-physical model ............................................................... 61
  4.2.3 Cyber-Attack Simulation ............................................................ 63
4.3 Severity Classification .................................................. 71
  4.3.1 Kundur Power System Model ...................................... 71
  4.3.2 Australian Power System Model ................................. 74

Chapter 5 CONCLUSION AND FUTURE WORK ....................... 76
  5.1 Future Work .......................................................... 78

BIBLIOGRAPHY .................................................................. 80

APPENDIX .......................................................................... 86
  Appendix A Model Parameters ............................................ 87
    A.1 IEEE Standard Kundur Power System Model ................. 87
**LIST OF TABLES**

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 4.1</td>
<td>Load Flow results for Kundur power system model</td>
<td>47</td>
</tr>
<tr>
<td>Table 4.2</td>
<td>Network Links in network architecture of IEEE Kundur 4-machine model</td>
<td>51</td>
</tr>
<tr>
<td>Table 4.3</td>
<td>Classification of $J$ into discrete bins</td>
<td>71</td>
</tr>
<tr>
<td>Table A.1</td>
<td>Generator Parameters for the 4-machine 2-Area Kundur Model</td>
<td>88</td>
</tr>
</tbody>
</table>
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure Number</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Generator $G_i$ supplying power to load $L_k$</td>
<td>13</td>
</tr>
<tr>
<td>2.2</td>
<td>$n$-bus power system network with full connectivity</td>
<td>16</td>
</tr>
<tr>
<td>2.3</td>
<td>Power grid cyber-physical infrastructure</td>
<td>26</td>
</tr>
<tr>
<td>2.4</td>
<td>Cyber-physical network architecture of a wide-area power system</td>
<td>27</td>
</tr>
<tr>
<td>4.1</td>
<td>Single line diagram of Kundur’s Two-Area system</td>
<td>46</td>
</tr>
<tr>
<td>4.2</td>
<td>Closed loop response of the discrete-time system</td>
<td>48</td>
</tr>
<tr>
<td>4.3</td>
<td>Excitation control inputs to the machines of the discrete-time system</td>
<td>48</td>
</tr>
<tr>
<td>4.4</td>
<td>Closed loop response of the discrete-time system with network delays</td>
<td>49</td>
</tr>
<tr>
<td>4.5</td>
<td>Excitation control inputs to the machines of the discrete-time system</td>
<td>50</td>
</tr>
<tr>
<td>4.6</td>
<td>Kundur Model - Phase angles plots at all generator buses for systems with and without DoS Attack</td>
<td>52</td>
</tr>
<tr>
<td>4.7</td>
<td>Kundur Model - Variation of $J$ when the security attack is between link connecting generators G1-G2 and strategy I is implemented</td>
<td>53</td>
</tr>
<tr>
<td>4.8</td>
<td>Kundur Model - Variation of $J$ when the security attack is between link connecting generators G1-G2 and strategy II is implemented</td>
<td>54</td>
</tr>
<tr>
<td>4.9</td>
<td>Kundur Model - Variation of $J$ when the security attack is between link connecting generators G3-G4 and strategy I is implemented</td>
<td>55</td>
</tr>
<tr>
<td>4.10</td>
<td>Kundur Model - Variation of $J$ when the security attack is between link connecting generators G3-G4 and strategy II is implemented</td>
<td>55</td>
</tr>
<tr>
<td>4.11</td>
<td>Kundur Model - Variation of $J$ when the security attack is between link connecting generators G1-G3 and strategy I is implemented</td>
<td>56</td>
</tr>
<tr>
<td>4.12</td>
<td>Kundur Model - Variation of $J$ when the security attack is between link connecting generators G1-G3 and strategy II is implemented</td>
<td>56</td>
</tr>
<tr>
<td>4.13</td>
<td>Kundur Model - Variation of $J$ when the security attack is between link connecting generators G1-G4 and strategy I is implemented</td>
<td>57</td>
</tr>
<tr>
<td>4.14</td>
<td>Kundur Model - Variation of $J$ when the security attack is between link connecting generators G1-G4 and strategy II is implemented</td>
<td>57</td>
</tr>
<tr>
<td>4.15</td>
<td>Kundur Model - Variation of $J$ when the security attack is between link connecting generators G2-G3 and strategy I is implemented</td>
<td>58</td>
</tr>
<tr>
<td>4.16</td>
<td>Kundur Model - Variation of $J$ when the security attack is between link connecting generators G2-G3 and strategy II is implemented</td>
<td>58</td>
</tr>
<tr>
<td>4.17</td>
<td>Kundur Model - Variation of $J$ when the security attack is between link connecting generators G2-G4 and strategy I is implemented</td>
<td>59</td>
</tr>
<tr>
<td>4.18</td>
<td>Kundur Model - Variation of $J$ when the security attack is between link connecting generators G2-G4 and strategy II is implemented</td>
<td>59</td>
</tr>
<tr>
<td>4.19</td>
<td>Single line diagram of 14-machine 4-Area, Australian power system</td>
<td>60</td>
</tr>
</tbody>
</table>
Figure 4.20 Closed loop response of the discrete-time system ................. 62
Figure 4.21 Excitation control inputs to the machines of the discrete-time system 62
Figure 4.22 Closed loop response of the discrete-time system with network delays 63
Figure 4.23 Excitation control inputs to the machines of the discrete-time system with network delays .............................................................. 64
Figure 4.24 Australian Power System - Phase angles plots at all generator buses for system with and without DoS Attack. ......................... 66
Figure 4.25 Australian power grid - Variation of $J$ when the security attack is between link connecting generators G9-G10 and strategy I is implemented. ................................. 67
Figure 4.26 Australian power grid - Variation of $J$ when the security attack is between link connecting generators G9-G10 and strategy II is implemented. ........................................ 68
Figure 4.27 Australian power grid - Variation of $J$ when the security attack is between link connecting generators G1-G11 and strategy I is implemented. ............................... 68
Figure 4.28 Australian power grid - Variation of $J$ when the security attack is between link connecting generators G1-G11 and strategy II is implemented. ............................... 68
Figure 4.29 Australian power grid - Variation of $J$ when the security attack is between link connecting generators G2-G7 and strategy I is implemented. ............................... 69
Figure 4.30 Australian power grid - Variation of $J$ when the security attack is between link connecting generators G2-G7 and strategy II is implemented. ............................... 69
Figure 4.31 Kundur-Model -Strategy I - Decision tree classifier. Classifies the cost function of strategy I into 4 classes based on the severity ............. 73
Figure 4.32 Kundur Model - Strategy II - Decision tree classifier. Classifies the cost function of strategy II into 4 classes based on the severity ............. 73
Figure 4.33 Australian Power System - Strategy I - Decision tree classifier. Classifies the cost function of strategy I into 4 classes based on the severity ...................... 74
Figure 4.34 Australian Power System - Strategy II - Decision tree classifier. Classifies the cost function of strategy II into 4 classes based on the severity ...................... 74

viii
Large-scale network dynamic systems (NDS) or cyber-physical systems (CPS) play an ubiquitous role in the study of the numerous physical and engineering systems such as robotics [1], computer networks [2], sensor networks [3], unmanned vehicles [4], and electric power systems [5]. Over the past decade tremendous research devoted to these studies has developed the theoretical foundation for modeling, monitoring and control of typical linear and non-linear NDS [4].

Most power systems on the level of a continent are interconnected (such as in Europe
or in North America) giving a gigantic dimension to this system, whereas its control still remains limited in scale. For decades, traditional power system operation and control has been performed by systems built with a centralized architecture, using Supervisory Control and Data Acquisition (SCADA) systems and Energy Management System (EMS). These systems were initially developed in the 1970s, and as they were limited to low computational power and communication network bandwidth available at that time, they were designed to collect measurements at a data rate on the order of seconds [6]. Due to these low data rates, SCADA systems are only able to provide snapshots of the power system in steady state rather than capturing the power system dynamics in real-time [7, 8]. SCADA/EMS solutions have performed well in the traditional power system operation and control where sufficient security margins and reserves are available. However, due to the increasing connection of power sources providing intermittent generation, increasing consumption, increasing interconnection of national grids, and regulatory constraints on the deployment of new lines, modern power systems tend to operate much closer to their limitations than they used to. There have been five massive blackouts over the past 40 years, three of which have occurred in the past decade. More blackouts and brownouts are occurring due to the slow response times of the mechanical switches, a lack of automated analytics, and "poor visibility" - a lack of situational awareness on the part of grid operators. These concerns along with the development in Information and Communication Technology (ICT) have resulted in recent paradigm shift to smart grid power system infrastructures [9].

The smart grid refers to the next-generation electrical power grid that aims to provide reliable, efficient, secure, and quality energy generation/distribution/consumption using modern information, communications, and electronics technology. The smart grid will
introduce a distributed and user-centric system that will incorporate end-consumers into its decision processes to provide a cost-effective and reliable energy supply. The modern infrastructure will play a vital role in managing, controlling, and optimizing different devices and systems in smart grids. Unlike the existing electrical power grid, smart grid will use two-way data communication technologies to integrate the utility control system with end-users and consumers, so that intelligent power generation, control, and consumption can be achieved [10].

1.1 Wide-Area Measurement and Control

One key component of smart grid development over the past decade is the deployment of measurement and instrumentation systems, especially in the form of the Wide-Area Measurement Systems (WAMS) and Wide-Area Control Systems (WACS) technologies [11, 12]. Sophisticated digital recording devices called Phasor Measurement Units or PMUs are currently being installed at different points in the North American grid, especially under the smart grid initiatives of the US Department of Energy. These devices record and communicate GPS-synchronized, high sampling rate (6-60 samples/sec), dynamic power system data [13]. These features allow the operators to observe power system dynamics in real-time and to correlate power system events globally.

The idea of wide-area control rests upon transmission of real-time dynamic measurements of voltage, phase angle, and frequency from PMUs located at different buses in a grid as feedback variables to controllers that may be geographically distant from the PMUs. Although synchrophasor technology has been available since the 1980s, its deployment
has been highly constrained by the limited capabilities of the underlying ICT infrastructure at the time, including the limited communication bandwidth and computational power. Research platforms such as the North American Synchrophasor Initiative (NASPI) [14] and the Western Interconnection Synchrophasor Project (WISP) [15] have been formed to track the dynamic health of the geographically dispersed large power networks [16]. The data is transferred through a wide-area communication network, which in the current state-of-art is a shared network running multiple applications, and thereby incurring noticeable network delays arising due to transport, routing, and queuing. Yet another source of delay, which unlike the previous three is a malicious consequence, is Denial-of-Service (DoS) attacks on the communication links carrying the PMU measurements from one location to another.

1.2 Motivation of the Study

In a smart grid architecture there is a heavy dependence on information networking, which inevitably surrenders the smart grid to potential vulnerabilities associated with communications and networking systems. This in fact increases the risk of compromising reliable and secure power system operation, which, nonetheless, is the ultimate objective of the smart grid. From [17–19], we can see that potential network intrusion by adversaries may lead to a variety of severe consequences in the smart gird, ranging from customer information leakage to a cascade of failures, such as massive blackout and destruction of infrastructure.

As a result, we are motivated to investigate the security issues in the wide-area control implementation in a smart grid. In this work, we study the impacts of Denial-of-Service
1.3. LITERATURE REVIEW

(DoS) attacks on the cyber-physical power system. Since the research on cyber-security for wide-area systems is still in its early stages our objective is, firstly to derive a nominal small-signal model of the power system network considering its swing and excitation dynamics, and secondly to develop a delay-aware Linear Quadratic Regulator (LQR) controller without considering any DoS. Thereafter, we study the impacts of Dos on the LQR controller performance and propose two mitigation strategies to reduce the negative effects of the DoS attack.

1.3 Literature Review

The recent developments of ICTs at reasonable cost offers possible solutions for electrical system that were unimaginable only a few years ago. Thus, the possibility of installing Intelligent Electronic Devices (IEDs) with bi-directional communication with the network at the site of the end user or load is changing the future vision of these networks. Since the inception of smart grid solutions for the shortcomings of traditional power grid, a lot of research has been conducted on smart grid infrastructure and networking. In modern power systems, wide-area measurement and control systems have been applied for various issues such as stability, security assessment and enhancement [20].

A considerable amount of research has been conducted on possible applications of synchrophasors. Out of these applications most of them focus on monitoring and situational awareness with a few applications in the control area [12]. PMU can measure the amplitude and phase angle of the voltage of the nodes where PMUs are installed directly. For on-line applications, this could replace the iteration process of power flow calculation
1.3. LITERATURE REVIEW

and state estimation [21, 22]. The precision of PMU measurements is very high and this can be combined with existing SCADA system to increase the precision of power system state estimation [23]. In [24], a power system harmonic state estimation based on phasor measurements has been proposed to transform the harmonic state estimation of the whole power system into state estimation of many single-bus systems.

Application of wide-area measurements for control purposes is still mostly in theoretical discussions rather than practical implementation. In WAMS, the dynamic real-time operation state of power system can be used as the initial condition for existing methods, such as Extended Equal Area Criteria (EEAC), Auto-Regression (AR) method, and so on. Once real-time WAMS data is readily available, transient stability control would be one of the important WAMS applications in the future [25, 26].

Depending on oscillation scale and the number of generators oscillating with each other, power system oscillation can be divided into local intra-area oscillation mode and inter-area oscillation mode. By using the real-time synchropasor data, various identification algorithms such as characteristic equation, recursive least squares, least mean squares, prony method, and AR method, Kalman filter technique have been proposed to estimate the oscillation parameters. In [27], a small signal stabilization controller with Power System Stabilizer (PSS) was proposed. Once oscillations were detected from the WAMS data, Static Var Compensators (SVCs) and Thyristor Controlled Series Capacitors (TCSCs) installed on important tie lines would be used to suppress the power oscillations. Case study showed that black out in USA on 10 Aug 1966 could be prevented by the proposed control scheme.

Majority of the ongoing NASPI-net activities are devoted to the hardware planning aspects of the communication [28, 29]. Only a modest effort has been made so far to study
the impact of delays [30, 31], with typical approach being to design a nominal controller and testing its robustness and sensitivity to the worst-case delays. In [30], the impact of time delay on robust wide area controller design in a two-area four machine power system is studied. From the simulations, it is found that the overshoot value of active power variation increases and the settling time is lengthened when time delay occurs. In [31], To address the problems posed by the time-delays on a cyber-physical system control [32] proposes an Arbitrated Networked Control Systems (ANCS) in order to emphasize that the control systems are to be designed for networks that are scheduled or arbitrated.

In [33], a method for optimizing the amount of platform resources required to ensure stability of the control system via a buffer control mechanism that exploits the ability of drop signals to the control systems and an associated analysis of the drop bound, is proposed. In [34], a delay-aware LQR controller for a wide-area power system is designed by exploiting the flexibility and transparencies of the communication network such as scheduling policies, bandwidth to co-design a delay-aware state feedback control law. The enhancement in the overall closed loop performance of the system compared to traditional robust controller is illustrated with a 50-bus, 14-generator, 4-area power system model.

As the interaction between the physical and cyber systems increases, the physical systems become more susceptible to the security vulnerabilities in the cyber system. [35] investigates the security challenges and issues of CPS. For example, some hackers have broken into the air traffic control mission-support systems of the U.S. Federal Aviation Administration several times in recent years, according to an Inspector General report sent to the FAA in May, 2009 [36]. Some hackers are also able to hack those medical devices implanted in human body which have wireless communication [37]. A CIA report [38]
reveals that hackers have penetrated power systems in several regions outside the United States, and in at least one case caused a power outage affecting multiple cities. In 2010, the attackers demonstrated a software tool called CarShark [39] which could kill a car engine remotely, turn off the brakes so the car would not stop and make instruments give false readings by monitoring communications between the electronic control units (ECUs) and insert fake packets of data to carry out attacks. Hackers have designed a virus which can successfully attack Siemens plant-control system [40].

In [35] the security attacks are classified into four types. (1) Eavesdropping - refers to the attack that adversary can intercept any information communicated by the system [41]. It is called passive attack since the attacker does not interfere with the working of the system and simply observes its operation. (2) Compromised-Key Attack : A key is a secret code which is necessary to interpret secure information. Once an attacker obtains a key, then the key is considered a compromised key [42]. An attacker can gain access to a secured communication without the perception of sender or receiver by using the compromised key. (3) Man-in-the-Middle Attack - false messages are sent to the operator, and can take form of a false negative or false positive. This may cause the operator to take an action, such as flipping a breaker, when it is not required which causes undesirable results. (4) Denial-of-Service Attack (Dos) - is one of the most common network attacks that prevent the legitimate traffic or requests for network resources from being processed or responded by the system. These type of attacks usually transmits a huge amount of data to the network to make it busy handling the junk data so that the normal services cannot be provided.

In recent years research efforts have been taken in the direction of building the security of the CPS. In [43], the fundamental monitoring limitations are characterized from a
system-theoretic and graph-theoretic perspective. Further a centralized and distributed attack detection and identification monitors are designed. In [44] denial-of-service against a networked control system is defined and a counter measure based on semi-definite programming is proposed. In [45], the effect of replay attacks on a control system is discussed. Replay attacks are cast by hijacking the sensors, recording the readings for a certain amount of time, and repeating such readings while injecting an exogenous signal into the system. It is shown that these attacks can be detected by injecting a signal unknown to the attacker into the system. In [46], a resilient control problem is studied, in which control packets transmitted over a network are corrupted by a human adversary. A receding-horizon Stackelberg control law is proposed to stabilize the control system despite the attack.

1.4 Organization of Thesis

This thesis has been organized as per the following chapters:

- **Chapter 2**: Wide-Area LQR Control
  The second chapter presents the mathematical model of the wide area power system and defines the control objective of the dynamic system. First, considered a third order small-signal model of the synchronous generators network in a wide area power system and represented them as state space model. Second, we derive the corresponding model for a system with network delays due to the cyber-physical infrastructure. Finally we define the optimal control objective and design a LQR controller for the cyber-physical wide-area power system.

- **Chapter 3**: Denial of Service Attacks and Mitigation Strategies
The third chapter covers the potential cyber-security threats of a shared wide-area power system network. We describe the three security attack parameters and design simulation experiments based on the attack parameters. Thereafter, we propose two mitigation strategies for DoS attack scenarios, and finally based on the performance criteria measured we classify the severity of the attack with a decision tree classifier.

• **Chapter 4: Simulation and Results**

The fourth chapter presents the simulation data and results of DoS attacks on (1) 4-machine 2-area IEEE standard Kundur model and (2) 50-bus, 14-machine Australian power system. For this simulation we used MATLAB and C++ to collect performance criteria data for various experiments for the proposed mitigation strategies. We have designed decision tree classifier for each strategy using Matlab statistic toolbox.

• **Chapter 5: Conclusion and Future Work**

The fifth chapter summarizes the impact of DoS attacks on a wide-area power system covered in this thesis, reviews the results and draws conclusions based on the simulation results. Future work in the area of Wide-Area Control design and cyber-security is suggested.
2.1 Dynamic Model of a Power System

2.1.1 Synchronous Generator Models

Consider a power system network with $n$ buses. Without loss of generality, classify the first $n_1$ buses to be generator buses, meaning that these buses are directly connected to a synchronous generator operating at a steady-state frequency of 60 Hz or $120\pi$ radians/second,
and the remaining \((n - n_1)\) buses as load buses meaning that active and reactive power are extracted from these buses in the form of loads. The schematic diagram of the \(i^{th}\) generator \(G_i\) supplying power to the \(k^{th}\) load through a transmission line is shown in Fig. 2.1a, and its corresponding circuit diagram is shown in Fig. 2.1b. Since this is an AC power system, the voltages and currents in the network will be complex numbers, each denoted by a magnitude and phase angle. The voltage at the \(i^{th}\) bus is denoted as \(V_i = V_i \angle \theta_i\), where \(V_i\) is the magnitude (volts) and \(\theta_i\) is the phase (radians). The internal voltage phasor of a synchronous generator connected to any generator bus is denoted as \(\hat{E}_i = E_i \angle \delta_i\), as shown in Fig. 2.1b. Each synchronous generator may be modeled by a set of third-order differential algebraic equations [47, 48]

\[
\dot{\delta}_i = \omega_i - \omega_s \tag{2.1}
\]

\[
M_i \dot{\omega}_i = P_{mi} - D_i (\omega_i - \omega_s) - P_i^G \tag{2.2}
\]

\[
\tau_i \dot{E}_i = -\frac{x_{di}'}{x_{di}} + \frac{x_{di}'}{x_{di}} V_i \cos(\delta_i - \theta_i) + \hat{E}_i 
\tag{2.3}
\]

\[
P_i^G = \frac{e_i V_i}{x_{di}} \sin(\delta_i - \theta_i) + \frac{x_{d}'}{2x_{d1}x_{d2}} V_i^2 \sin(2(\delta_i - \theta_i)) \tag{2.4}
\]

\[
Q_i^G = \frac{e_i V_i}{x_{di}} \cos(\delta_i - \theta_i) - \frac{x_{q}'}{2x_{d1}x_{d2}} - \frac{x_{q}'}{2x_{d1}x_{d2}} \cos(2(\delta_i - \theta_i)) V_i^2 \tag{2.5}
\]

where, the states \(\delta_i, \omega_i\) and \(E_i\) are respectively, the generator phase angle (radians), angular velocity of the rotor (rad/sec) and quadrature-axis internal emf; \(\omega_s\) is the synchronous frequency of \(120\pi\) radians/sec; \(P_i^G\) and \(Q_i^G\) are respectively, the active and reactive power produced by the \(i^{th}\) generator (Mega Watts and Mega VAR), \(M_i\) is the inertia constant (seconds), \(D_i\) is the generator damping, \(P_{mi}\) is the mechanical power input to the \(i^{th}\) turbine.
2.1. DYNAMIC MODEL OF A POWER SYSTEM CHAPTER 2. WIDE AREA LQR CONTROL

(a) Schematic diagram

(b) Circuit diagram

Figure 2.1 Generator $G_i$ supplying power to load $L_k$

(Mega Watts). $\tau_i$ is the excitation time constant (seconds); $x_{d_i}$, $x'_{d_i}$ and $x_{q_i}$ are the direct-axis salient reactance, direct-axis transient reactance and quadrature-axis salient reactance (all in ohms), respectively. The variables $V_i$ and $\theta_i$ are algebraic variables, meaning that they are not direct state variables but only algebraic functions of the state variables that follow from Eq. 2.4-Eq. 2.5. The control variable is the field voltage $E_{Fi}$, which can be split into two separate terms

$$E_{Fi} = \hat{E}_{Fi} + E_i$$

(2.6)
where, the first term is a constant that fixes the equilibrium value, and the second is a
designable control input that can be applied via state feedback or output feedback. This
input is commonly referred to as excitation control. Detailed description of the various
parameters of the model, Eq. 2.1-Eq. 2.5 can be found in [47]. Illustrative examples of
excitation control designs can be found in [49, 50].

More detailed models of synchronous generator such as the $9^{th}$-order model describing
the electromagnetic dynamics of the stator can be found in literature [50]. These states
are classified as fast states, meaning that their time-scale of evolution is in the order of
milliseconds [51]. The objective of wide-area control, however is to control oscillation
components that arise out of local and inter-area oscillations, the spectrum for which lie
between 0.1 Hz to 1 Hz. Therefore, we have limited to a third order models.

2.1.2 Load Models

The active and reactive power drawn by the $j^{th}$ load, where $j = n_1 + 1, n_2 + 2, \ldots , n$, can be
modeled as [49]

$$P_j^L = a_j V_j^2 + b_j V_j + c_j \quad (2.7)$$

$$Q_j^L = e_j V_j^2 + f_j V_j + g_j \quad (2.8)$$

where, $(a_j, b_j, c_j)$ and $(e_j, f_j, g_j)$ are load-specific constant coefficients of appropriate di-
mension, and the three terms in each equation explicitly represent the contribution of each
type of load, namely, constant current and constant power load, respectively.
2.1.3 Transmission Line Models

A transmission line connecting the \(i^{th}\) bus (sending end) to the \(j^{th}\) bus (receiving end) is modeled by a standard lumped parameter pi-model, where the active and reactive powers transferred across the line are given as \([49, 50]\)

\[
P_{ij} = G_{ij} V_i^2 + B_{ij} V_i V_j \sin(\theta_i - \theta_j) - G_{ij} V_i V_j \cos(\theta_i - \theta_j) \tag{2.9}
\]

\[
Q_{ij} = (B_{ij} - B_{ij}^c) V_i^2 - B_{ij} V_i V_j \cos(\theta_i - \theta_j) - G_{ij} V_i V_j \sin(\theta_i - \theta_j). \tag{2.10}
\]

Here, \(G_{ij} = G_{ji}\) is the line conductance, \(B_{ij} = B_{ji}\) is the line series susceptance, and \(B_{ij}^c = B_{ji}^c\) is the line shunt susceptance connecting bus \(i\) to bus \(j\), all in mhos. If bus \(i\) and bus \(j\) are not connected then all the three quantities are zero.

2.1.4 Network Dynamic Models

Equations Eq. 2.1-Eq. 2.2 follows from Newton’s second law of motion applied to the internal states of the \(i^{th}\) generator. The algebraic variables at any bus, however, follow Kirchoff’s law manifesting in the form of active and reactive power balance

\[
0 = \sum_{k \in \mathcal{N}_i} P_{ik} - P^L_i, \quad 0 = \sum_{k \in \mathcal{N}_i} Q_{ik} + Q^L_i, \quad i = n_1 + 1, n_1 + 2, \ldots, n \tag{2.11}
\]

\[
0 = \sum_{k \in \mathcal{N}_j} P_{jk} - P^L_j, \quad 0 = \sum_{k \in \mathcal{N}_j} Q_{jk} + Q^L_j, \quad j = n_1 + 1, n_1 + 2, \ldots, n \tag{2.12}
\]

where, \(\mathcal{N}_i\) denotes the set of bus numbers that are connected to bus \(i\), i.e., the neighbor set of bus \(i\). The dynamical model for the entire system can be constructed by relating the
Figure 2.2 $n$-bus power system network with full connectivity

generator models, load models and transmission line models over any given interconnection of the $n$ buses making use of the power balance equations Eq. 2.11-Eq. 2.12. To achieve this in the most generic way, consider the network to be of the form shown in Fig. 2.2, where each of the $n$ buses is assumed to be connected to a generator as well as to a load, and every bus is assumed to be connected to every other bus. The transmission lines are assumed to have both resistance and reactance, and are modeled by pi-models. If in reality, any two buses are not connected then the corresponding line impedance must be substituted by
2.1. Dynamic Model of a Power System Chapter 2. Wide Area LQR Control

infinity (or, equivalently the line admittance by zero). If any bus \( i \) does not have any load extracted from it then the load powers \( P_i^L \) and \( Q_i^L \) must simply be substituted as zero. If any bus \( i \) does not have a generator connected to it then \( M_i \) may be substituted as zero, and \( x_{di}, x_{di} \) and \( x_{qi} \) must all be substituted as infinity.

2.1.5 Small-Signal Model

Next, consider a small perturbation over an existing equilibrium \((\delta_{i0}, \omega_s, E_{i0}, V_{i0}, \theta_{i0}), i = 1, \ldots, n\). From Eq. 2.4 the change in the active power flowing out of the \( i^{th} \) generator can be written as

\[
\Delta P_i^G = C_{1i} \Delta E_i + C_{2i} \Delta V_i + C_{3i} \Delta \delta_i + C_{4i} \Delta \theta_i
\]  

(2.13)

where,

\[
C_{1i} = \frac{V_{i0} \sin(\delta_{i0} - \theta_{i0})}{x_{di}^{'}}
\]  

(2.14)

\[
C_{2i} = \frac{E_{i0} \sin(\delta_{i0} - \theta_{i0}) + 2 Y_{2i} V_{i0} \sin(2(\delta_{i0} - \theta_{i0}))}{x_{di}^{'}}
\]  

(2.15)

\[
C_{3i} = \frac{E_{i0} V_{i0} \cos(\delta_{i0} - \theta_{i0}) + 2 Y_{2i} V_{i0}^2 \cos(2(\delta_{i0} - \theta_{i0}))}{x_{di}^{'}}
\]  

(2.16)

\[
C_{4i} = \frac{-E_{i0} V_{i0} \cos(\delta_{i0} - \theta_{i0}) + 2 Y_{2i} V_{i0}^2 \cos(2(\delta_{i0} - \theta_{i0}))}{x_{di}^{'}}
\]  

(2.17)

\[
Y_{2i} = \frac{x_{di}^{' - x_{qi}}}{2 x_{d1}^{' x_{qi}^{'}}}
\]  

(2.18)

The algebraic variables can be related to the states using Kirchhoff current law (KCL) at every bus. Let the current flowing out of the \( i^{th} \) generator be \( \hat{I}_{Gi} \), the current extracted by the load at the \( i^{th} \) bus be \( \hat{I}_{Li} \), and the total current flowing out of the \( i^{th} \) bus to the rest of
the network be $\hat{I}_{Ni}$. If the current flows into this bus then its sign will be negative. At any instant of time $t$, application of KCL at this bus yields

$$\hat{I}_{Gi}(t) = \hat{I}_{Li}(t) + \hat{I}_{Ni}(t). \quad (2.19)$$

Since the laws of electricity hold true for instantaneous values of the electrical variables at any instant of time, from now onwards the argument $t$ will be dropped for all variables.

$$\hat{I}_{Gi} = \left( \frac{P_i + jQ_i}{V_i} \right)^* \quad (2.20)$$

where, $^*$ denotes complex conjugate. Extending Eq. 2.19 to all $n$ buses leads to

$$\hat{I}_G = \hat{I}_L + \hat{I}_N \quad (2.21)$$

where $\hat{I}_G = col(\hat{I}_{G1}, \ldots, \hat{I}_{Gn})$, $\hat{I}_L = col(\hat{I}_{L1}, \ldots, \hat{I}_{Ln})$, and $\hat{I}_N = col(\hat{I}_{N1}, \ldots, \hat{I}_{Nn})$. It follows from Ohm’s law that

$$\hat{I}_G = Y_g(\hat{E} - \hat{V}) \quad (2.22)$$

where, $Y_g = diag(1/x_{d1}^i)$, and $\hat{E}$ and $\hat{V}$ are the vectors of all generator voltage phasors and bus voltage phasors, respectively. By applying KCL at the buses, the network flows can similarly be written as

$$\hat{I}_n = Y_{bus} \hat{V} \quad (2.23)$$

where, $Y_{bus}$ is the bus admittance matrix. Considering that the admittance of the trans-
mission line connecting bus \(i\) and bus \(k\) is \(z_{ik} = r_{ik} + jx_{ik}, \ j = \sqrt{-1}\), the structure of \(Y_{bus}\) follows as:

\[
Y_{bus,ik} = \frac{1}{r_{ik} + jx_{ik}}, \text{ if bus } i \text{ and bus } k \text{ are connected} 
\]

(2.24)

\[
Y_{bus,ik} = 0, \text{ if bus } i \text{ and bus } k \text{ are not connected} 
\]

(2.25)

\[
Y_{bus,ii} = -\sum_{k=1,k\neq i}^{n} Y_{bus,ik} 
\]

(2.26)

From Eq. 2.21, Eq. 2.22, and Eq. 2.23 we obtain,

\[
\hat{V} = Y_1 \hat{E} + Y_2 \hat{I}_L 
\]

(2.27)

where, \(Y_1 = (Y_g + Y_{bus})^{-1} Y_g\), and \(Y_2 = (Y_g + Y_{bus})^{-1}\). Since elements of both \(Y_1\) and \(Y_2\) are complex numbers, they can be decomposed as

\[
Y_1 = Y_{R1} + jY_{I1}, \ Y_2 = Y_{R2} + jY_{I2} 
\]

(2.28)

Eq. 2.27 is in the phasor form, and needs to be decomposed into real and imaginary parts to extract the algebraic variables \(V\) and \(\theta\), as follows. Let

\[
\hat{V} = V_R + jV_I 
\]

(2.29)

\[
\hat{E} = E_R + jE_I 
\]

(2.30)

\[
\hat{I}_L = I_{LR} + jI_{LI} 
\]

(2.31)
so that Eq. 2.27 can be rewritten as

$$V_R = Y_{R1}E_R - Y_{I1}E_I + Y_{R2}I_{LR} - Y_{I2}I_{LI} \tag{2.32}$$

$$V_I = Y_{R1}E_I - Y_{I1}E_R + Y_{R2}I_{LI} + Y_{I2}I_{LR} \tag{2.33}$$

where,

$$V_R = \cos(V_1 \cos(\theta_1), V_2 \cos(\theta_2), \ldots, V_n \cos(\theta_n)) \tag{2.34}$$

$$V_I = \cos(V_1 \sin(\theta_1), V_2 \sin(\theta_2), \ldots, V_n \sin(\theta_n)) \tag{2.35}$$

$$E_R = \cos(E_1 \cos(\theta_1), E_2 \cos(\theta_2), \ldots, E_n \cos(\theta_n)) \tag{2.36}$$

$$E_I = \cos(E_1 \sin(\theta_1), E_2 \sin(\theta_2), \ldots, E_n \sin(\theta_n)) \tag{2.37}$$

The vectors $I_{LR}$ and $I_{LI}$ can be similarly defined by considering the real and imaginary parts of the load currents. Linearization of Eq. 2.32-Eq. 2.33 about the given equilibrium results in

$$\Delta V_R = Y_{R1}\Delta E_R - Y_{I1}\Delta E_I + Y_{R2}\Delta I_{LR} - Y_{I2}\Delta I_{LI} \tag{2.38}$$

$$\Delta V_I = Y_{R1}\Delta E_I - Y_{I1}\Delta E_R + Y_{R2}\Delta I_{LI} + Y_{I2}\Delta I_{LR} \tag{2.39}$$
where from Eq. 2.34-Eq. 2.37 it follows that

\[
\Delta V_R = diag_{i=1(1)\mathrm{n}}(\cos(\theta_{i0}))\Delta V - diag_{i=1(1)\mathrm{n}}(V_{i0}\sin(\theta_{i0}))\Delta \theta
\]  
(2.40)

\[
\Delta V_I = diag_{i=1(1)\mathrm{n}}(\sin(\theta_{i0}))\Delta V + diag_{i=1(1)\mathrm{n}}(V_{i0}\cos(\theta_{i0}))\Delta \theta
\]  
(2.41)

\[
\Delta E_R = diag_{i=1(1)\mathrm{n}}(\cos(\delta_{i0}))\Delta E - diag_{i=1(1)\mathrm{n}}(E_{i0}\sin(\delta_{i0}))\Delta \delta
\]  
(2.42)

\[
\Delta E_I = diag_{i=1(1)\mathrm{n}}(\sin(\delta_{i0}))\Delta E + diag_{i=1(1)\mathrm{n}}(E_{i0}\cos(\delta_{i0}))\Delta \delta
\]  
(2.43)

Here, \(\Delta V = col(\Delta V_1, \Delta V_2, \ldots, \Delta V_n)\), \(\Delta \theta = col(\Delta \theta_1, \Delta \theta_2, \ldots, \Delta \theta_n)\), \(\Delta E = col(\Delta E_1, \Delta E_2, \ldots, \Delta E_n)\), and \(\Delta \delta = col(\Delta \delta_1, \Delta \delta_2, \ldots, \Delta \delta_n)\). Substituting Eq. 2.40-Eq. 2.43 in Eq. 2.38-Eq. 2.39 and a few simple calculations yield the exact expression of the algebraic variables in terms of the states as

\[
\begin{bmatrix}
\Delta V \\
\Delta \theta
\end{bmatrix} = \Pi^{-1} F\begin{bmatrix}
\Delta \delta \\
\Delta E
\end{bmatrix} + \Pi^{-1} \begin{bmatrix}
\Lambda_1 \\
\Lambda_2
\end{bmatrix} G
\]  
(2.44)

where,
2.1. DYNAMIC MODEL OF A POWER SYSTEM CHAPTER 2. WIDE AREA LQR CONTROL

\[ \Pi = \begin{bmatrix} \text{diag}(\cos(\theta_i)) & -\text{diag}(V_{i0}\sin(\theta_i)) \\ \text{diag}(\sin(\theta_i)) & -\text{diag}(V_{i0}\cos(\theta_i)) \end{bmatrix} \]  

(2.45)

\[ \Psi = \begin{bmatrix} \Psi_1 \\ \Psi_2 \\ \Psi_3 \\ \Psi_4 \end{bmatrix} \]  

(2.46)

\[ \Psi_1 := Y_{R1}\text{diag}(E_i\sin(\delta_{i0})) - Y_{I1}\text{diag}(E_i\cos(\delta_{i0})) \]  

(2.47)

\[ \Psi_2 := Y_{R1}\text{diag}(E_i\sin(\delta_{i0})) - Y_{I1}\text{diag}(\cos(\delta_{i0})) \]  

(2.48)

\[ \Psi_3 := Y_{R1}\text{diag}(E_i\sin(\delta_{i0})) - Y_{I1}\text{diag}(E_i\sin(\delta_{i0})) \]  

(2.49)

\[ \Psi_4 := Y_{R1}\text{diag}(\sin(\delta_{i0})) + Y_{I1}\text{diag}(\cos(\delta_{i0})) \]  

(2.50)

Next partition \( F \) into \((n \times n)\) blocks, and \( G \) into \((n \times 1)\) blocks as

\[ F = \begin{bmatrix} F_1 & F_2 \\ F_3 & F_4 \end{bmatrix}, \quad G = \begin{bmatrix} G_1 \\ G_2 \end{bmatrix} \]  

(2.51)

so that

\[ \Delta V = F_1 \Delta \delta + F_2 \Delta E + G_1 \]  

(2.52)

\[ \Delta \theta = F_3 \Delta \delta + F_4 \Delta E + G_2 \]  

(2.53)

Equations Eq. 2.52-Eq. 2.53 give the exact relationship of the algebraic variables and the state variables for the entire network. Next, linearize Eq. 2.2 about the given equilibrium, and use Eq. 2.13 to get
2.1. DYNAMIC MODEL OF A POWER SYSTEM  
CHAPTER 2. WIDE AREA LQR CONTROL

\[ M_i \Delta \dot{\omega}_i = \Delta P_{mi} - D_i \Delta \omega - (C_{1i} \Delta E_i + C_{2i} \Delta V_i + C_{3i} \Delta \delta_i + C_{4i} \Delta \theta_i) \]  
(2.54)

Similarly, linearize Eq. 2.3 about the given equilibrium to obtain

\[ \tau_i \Delta \dot{E}_i = a_i \Delta E_i + b_i \Delta V_i - e_i \Delta \delta_i + e_i \Delta \theta_i + \Delta E_i \]  
(2.55)

where, \( \Delta E_i \) denotes the designable excitation control input, and the constants \( a_i := -x_{di} / x_{di}' \), \( b_i := (x_{di} - x_{di}') \cos(\delta_i - \theta_i) / x_{di}' \), \( e_i := V_i (x_{di} - x_{di}') \sin(\delta_i - \theta_i) / x_{di}' \). From Eq. 2.52-Eq. 2.55, the overall linearized \((3n)^{th}\) order dynamic model of the network can finally be expressed as

\[
\begin{bmatrix}
\Delta \dot{\delta} \\
2H \Delta \dot{\omega} \\
T \Delta \dot{E}
\end{bmatrix}
= \begin{bmatrix}
0 & I & 0 \\
-L & -D & -P \\
K & 0 & J
\end{bmatrix}
\begin{bmatrix}
\Delta \delta \\
\Delta \omega \\
\Delta E
\end{bmatrix}
+ \begin{bmatrix}
0 \\
\cos l_{i=1(1)n}(\gamma_i) \\
\cos l_{i=1(1)n}(\rho_i)
\end{bmatrix}
\begin{bmatrix}
0 & I & 0 \\
I & 0 & 0 \\
0 & I & 0
\end{bmatrix}
\begin{bmatrix}
\Delta P_m \\
\Delta E_F
\end{bmatrix}
\]

(2.56)

where the various matrices on the RHS are given as follows:
2.1. DYNAMIC MODEL OF A POWER SYSTEM  

CHAPTER 2. WIDE AREA LQR CONTROL

\[ L = \begin{cases} 
L_{ik} = C_{2i}F_{1,ik} + C_{4i}F_{3,ik} & i \neq k \\
L_{ii} = C_{2i}F_{1,ii} + C_{3i} + C_{4i}F_{3,ii} 
\end{cases} \]  

(2.57)

\[ P = \begin{cases} 
P_{ik} = C_{2i}F_{2,ik} + C_{4i}F_{4,i} & i \neq k \\
P_{ii} = C_{2i}F_{2,ii} + C_{1i} + C_{4i}F_{2,ii} 
\end{cases} \]  

(2.58)

\[ K = \begin{cases} 
K_{ik} = b_i F_{1,ik} + e_i F_{3,ik} & i \neq k \\
K_{ii} = b_i F_{1,ii} - e_i + e_i F_{3,ii} 
\end{cases} \]  

(2.59)

\[ J = \begin{cases} 
J_{ik} = b_i F_{2,ik} + e_i F_{4,ik} & i \neq k \\
J_{ii} = b_i F_{2,ii} + a_i + e_i F_{4,ii} 
\end{cases} \]  

(2.60)

\[ \gamma_i = C_{2i}G_{1i} + C_{4i}G_{2i} \]  

(2.61)

\[ \rho_i = b_i G_{1i} + e_i G_{2i} \]  

(2.62)

\[ D = \text{diag}(D_i), \ M = \text{diag}(M_i), \ T = \text{diag}(\tau_i) \]  

(2.63)

and \( P_m := \text{col}_{i=1}^n(P_{mi}) \), \( E_F := \text{col}_{i=1}^n(E_{Fi}) \). Assuming PMUs are installed at designated buses whose indices are given by a set \( S \), the output equation can be formed as

\[ y = \text{col}_{i \in S}(\Delta V_i, \Delta \theta_i). \]  

(2.64)

These measured outputs will be used in the following sections for the purpose of monitoring the global dynamics of the power system and to design feedback control.

The Eq. 2.56 describes how the small-signal dynamic responses of voltages and phase
angles at various buses in a large power system following any fault or disturbance can be monitored and tracked in real-time using PMUs installed at those buses. Secondly, this state space is equation is used to formulate the wide-area control problem, for which Eq. 2.56-Eq. 2.64 will serve as the primary model indicating how the designable control inputs $\Delta P_m$ and $\Delta E_F$ enter the system dynamics.

The process of converting the original set of differential algebraic equations (DAEs) to the completely dynamic model Eq. 2.56 is referred to as the *Kron reduction*, further details can be found in [52, 53]. Depending on the type of load, the load-dependent terms $\gamma_i$ and $\rho_i$ may also be functions of $(\Delta V_i, \Delta \theta_i)$, and, therefore, functions of the states via Eq. 2.52-Eq. 2.53.

The continuous-time state-space of the linearized small-signal perturbation model of the wide-area power system can be represented as,

$$\dot{x}(t) = \mathcal{A}_c x(t) + \mathcal{B}_c u(t)$$

where, $x(t) = [\Delta \delta_1, \Delta \delta_2, \ldots, \Delta \delta_n, \Delta \omega_1, \Delta \omega_2, \ldots, \Delta \omega_n, \Delta E_1, \Delta E_2, \ldots, \Delta E_n]$, $\mathcal{A}_c$ and $\mathcal{B}_c$ are the system state and input matrices, respectively.

### 2.2 Power System with Delays

In a cyber-physical wide-area power system the states are measured using phasor measurement units (PMUs) and phasor data concentrators (PDCs) at different locations spread across multiple areas. The measurement data is transported using a shared network which induces a delays in the system. In this section we will first define the network architecture.
of the cyber physical system and then derive modified version of the linearized third order model of the power system obtained from Section 2.1.5 to accommodate the effects of the network delays.

2.2.1 Cyber-Physical System Architecture

![Power grid cyber-physical infrastructure](image)

Figure 2.3 Power grid cyber-physical infrastructure

Cyber-Physical Systems (CPS) are integration of computation, networking, and physical processes. Embedded computers and networks monitor and control the physical process, with feedback loops where physical processes affect computations and vice-versa. Fig. 2.3 shows a typical CPS view of the power grid. The cyber systems, consisting of electronic field devices, communication networks, substation automation systems, and control centers, are
embedded throughout the physical grid for efficient and reliable generation, transmission, and distribution of power. The control center is responsible for real-time monitoring, control, and operational decision making. Independent system operators (ISOs) perform coordination between power utilities, and dispatch commands to their control centers. Utilities that participate in power markets also interact with the ISOs to support market functions based on real-time power generation, transmission, and demand.

Figure 2.4 Cyber-physical network architecture of a wide-area power system
For our simulations and experiments we consider the network architecture as shown in Fig. 2.4. The architecture is assumed to consist of the following layers: (1) PMU measurements are first transmitted to a state estimator, which depending on the situation, may be centralized or distributed; the output of the state estimator at any time instant is the discrete-time state estimate of the swing and excitation states of all machines. (2) The state estimates are then transported to a third-party shared cloud computing network, where multiple virtual computers or machines (VM) are present. States of machines belonging to a specific balancing authority are stacked together and assigned to a specific VM. The VMs themselves may be physically present at different geographical locations, and are connected to each other through a wide-area communication network in the cloud. The VMs exchange state information through this network at every sampling instant, and each compute the LQR control input for the synchronous machines assigned to it at that sampling instant as a linear function of the states. (3) And, finally, the computed control input is transported back to the respective power system stabilizers in the grid for actuation. For this study we will assume that the communication links connecting the grid and the cloud are sufficiently secure, and hence DoS is only considered in the links connecting the VMs inside the cloud. The network between these VMs can be represented by a graph matrix, where $n$ is the number of VM nodes. If the link between nodes $i$ and $j$ exists, then $G(i, j) = 1$. Since LQR, in general, produces a full gain matrix (i.e., in general all entries of the gain matrix are non-zero), every VM, in general, must communicate with every other VM as a
result of which the graph matrix $G$ is represented as

$$G = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \vdots & \ddots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}_{n \times n}$$ (2.66)

### 2.2.2 System with Network delays

Since both the PMU measurements and the control inputs will be realized as discrete-time samples, we consider the discrete-time state-space equivalent of (2.56) as

$$x[k + 1] = Ax[k] + Bu[k]$$ (2.67)

where,

$$A = e^{\Delta \tau_j}, \quad B = \int_0^{\tau_j} e^{\Delta \tau_j} \mathcal{R} \, dt$$ (2.68)

$x[k]$ is $[\Delta \delta[k], \Delta \omega[k], \Delta E[k]]$, $u = [u_1, u_2, \ldots, u_n]$ models the excitation voltage inputs, $A$ is the discrete-time state matrix, $B$ is the discrete-time input matrix and $\tau_j$ is the sampling time of the PMUs.

In a public shared cloud network as shown in Fig. 2.4, multiple applications will be running in parallel, as a result of which the data traffic between the VMs will be subjected to congestion. The communication between the VMs which are geographically far apart will incur standard network delays due to transmission, queuing, propagation and routing. Due to these network delays the PMU measurements (states) of all the machines at any time instant $k$ are not readily available to the controllers (VMs) at time $t = k$. The states of $i^{th}$
machine arrives at every other node after a variable communication delay. The maximum delay threshold of a network is a characteristic of the communication network based on the bandwidth and length of network link. Let us assume $h$ seconds to be the maximum delay threshold of the communication network. This implies that in ideal conditions when all links are operational the states of the machines reach every other VM node within $h$ seconds. The control input cannot be evaluated until all the states are available, hence the control input for time instant $k$ will be available only at $t = k + h$. There will be a zero-order hold in control input at each node, and the control input for the period $t = [k, k + h)$. The effective control input $u_i(t)$ for a single sampling time duration $k < t < k + 1$ is represented by,

$$u_i[t] = \begin{cases} 
    u_i[k-1], & k < t < k + h \\
    u_i[k], & k + h < t < k + 1.
\end{cases} \quad (2.69)$$

Considering the control input from Eq. 2.69, the discrete-time state-space equation of the dynamic system with network delay threshold $h$ seconds can be rewritten as,

$$x[k+1] = Ax[k] + B_1 u[k-1] + B_2 u[k] \quad (2.70)$$

where,

$$B_1 = \int_0^{t=h} e^{A c t} B_c \, d t \quad (2.71)$$
$$B_2 = \int_h^{t=\tau} e^{A c t} B_c \, d t \quad (2.72)$$
By defining an augmented state $z[k] = [x[k] \ u[k-1]]^T$, (2.70) can be written as,

$$z[k+1] = \begin{bmatrix} A & B_1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x[k] \\ u[k-1] \end{bmatrix} + \begin{bmatrix} B_2 \\ I \end{bmatrix} u[k]$$

$$= \hat{A}z[k] + \hat{B}u[k] \tag{2.73}$$

Eq. 2.73 represents the state space model of a cyber-physical power system network and implement an LQR optimal controller for this model. The state $z[k]$ of the above mentioned system includes all the states from the discrete system without delays which are measured by the PMUs in network and the inputs to all the machines at the previous time instant $t = k - 1$.

2.3 LQR Control Design

The theory of optimal control is concerned with operating a dynamic system at minimum cost. Linear Quadratic Regulator (LQR) is a state feedback controller to optimize the quadratic cost function defined by the states and inputs of a linear system. For a discrete-time linear system defined by Eq. 2.73 and a quadratic cost function can be defined as

$$\min J = \sum_{k=0}^{\infty} z_k^T Q z_k + u_k^T R u_k$$

where $Q \geq 0$ and $R > 0$ are positive-semidefinite and positive-definite matrices, respectively. $Q$ is the state weighing matrix and $R$ is the input weighing matrix. The construction of $Q$ follows from the minimization of the power flows across the tie-lines [34]. The inputs to all
the generators are equally optimized and hence \( R \) is chosen to be identity. \( R \in \mathbb{R}^{n \times n} \) and \( Q \in \mathbb{R}^{4n \times 4n} \).

### 2.3.1 Optimizing the state cost \( Q \)

The \( Q \) for a network dynamic delay aware system, where the inputs from the previous time instant are augmented to the states of the system, can be represented as,

\[
Q = \begin{bmatrix} Q_{lq r} & 0 \\ 0 & R \end{bmatrix} \tag{2.75}
\]

\( Q_{lq r} \geq 0 \) should be chosen to achieve the following:

1. Minimize \( \Delta \omega(t) \) which is the deviation of the rotor velocities from the synchronous speed,

2. Minimize \( \Delta E \) : deviations of the quadrature-axis internal emf from their nominal values.

3. Minimize deviations of the active power inside each area to achieve minimum deviation of the phase difference \( (\Delta \delta_i - \Delta \delta_j) \), for any two generators \( i \) and \( j \) in the same area.

So we choose the \( x^T Q_{lq r} x \) as following

\[
x^T Q_{lq r} x = \sum_{i=1}^{P} \sum_{j=1}^{P} \alpha_{ij} (\Delta \delta_i - \Delta \delta_j)^2 + \sum_{j=1}^{n} (\beta_j \Delta \omega_i^2 + \gamma_j \Delta E_i^2) \tag{2.76}
\]

where \( \alpha_{ij}, \beta_j \) and \( \gamma_j \) are normalized weight coefficients, whose values depend on which
2.3. LQR CONTROL DESIGN

CHAPTER 2. WIDE AREA LQR CONTROL

states need to be penalized more than others for a given design problem. For our experiments we consider $\beta_j$ and $\gamma_j$ to be unity and $\alpha_{ij}$ can be given by,

$$
\alpha_{ij} = \begin{cases} 
1, & \text{if } i \neq j, \\
-\sum_{j=1}^{n} \alpha_{ij}, & \text{if } i = j.
\end{cases}
$$

(2.77)

The control input $u[k]$ from the control law is of the form,

$$
u[k] = -K_{lqr}z[k] = K_0x[k] + L_0u[k-1]
$$

(2.78)

where $K_{lqr}$ is given by,

$$
K_{lqr} = (R + B^T P B)^{-1}(B^T PA)
$$

(2.79)

and $P$ is the unique positive solution to the discrete-time algebraic Ricatti equation (DARE),

$$
P = A^T PA - (A^T PB)(R + B^T P B)^{-1}(B^T PA) + Q
$$

(2.80)

$K_{lqr} = [K_0 \ L_0]$ is the feedback gain matrix resulting from the LQR control design, $K_0 \in \mathbb{R}^{n \times 3n}$ and $L_0 \in \mathbb{R}^{n \times n}$. When implemented in a distributed network the control input of each synchronous generator is evaluated at a separate node with state measurements from all the generators. The control input $u_i$ of $i^{th}$ machine in a full graph network as mentioned above can be represented as,

$$
u_i[k] = (K_0 \circ G)_i x[k] + (L_0 \circ G)_i u[k-1]
$$

(2.81)
where, \( \mathcal{G} = [ G \mid G \mid G ] \) is the network graph matrix of the state measurements with \( G \) following from (2.66). \((K_0 \odot \mathcal{G})_i\) corresponds to the \( i^{th} \) row of the hadamard product of \( K_0 \) and \( \mathcal{G} \).
The security of Networked Control Systems (NCSs) naturally depends on the integration of cyber and physical dynamics and on different ways in which they are affected by the actions of human decision makers. Thus, problems in this area lie at the intersection of control systems and computer security [54]. As recently highlighted by the Maroochy water breach in March 2000 [55], multiple recent power blackouts in Brazil [56], the SQL Slammer worm attack on the Davis Besse nuclear plant in January 2003 [57], the StuxNet computer worm in June 2010 [58], and by various industrial security incidents [59], cyber-physical
systems are prone to failures and attacks on their physical infrastructure, and cyber attacks on their data management and communication layer.

First question for cyber-physical system security is whether NCS security can be handled simply with information technology (IT) and network security solutions. After all, NCSs are applications typically built on Internet Protocol (IP)-based networks. However, feedback loops inherent to NCSs and the coupling to the physical environment impose fundamentally new challenges for cybersecurity tools. NCSs highlight special feedback characteristics of control systems that have implications on the underlying physical dynamics. On one hand, the traditional IT security focuses on the protection of information in the cyberworld. On the other hand, classical control theory focuses on the attenuation of disturbances and uncertainties in the physical world. This separation was natural for many practical applications, such as traditionally hard-wired supervisory control and data acquisition (SCADA) systems. However, the separation at the design stages of IT security tools and control-theoretic implementations is no longer permissible. Indeed, NCSs are vulnerable to remote access over IP-based communication networks, software flaws and hardware malfunctions of off-the-shelf IT devices, and the presence of a large number of field devices used for sensing and actuation. In such a networked environment, the cyber and physical components become interconnected and hence, their security is interdependent [54].

Incorporating traditional IT security in control designs, such as encryption of certain communication channels is important; however, it is only a partial solution to NCS security concerns. Even if certain communication channels have been encrypted, malicious data or actions can enter due to unauthorized access to NCS components, which can result in undesirable behaviors of the controlled physical plant. Furthermore, many encryption
3.1. DENIAL-OF-SERVICE ATTACKS CHAPTER 3. CYBER ATTACKS AND MITIGATION

solutions will likely introduce time delay in the feedback loop, which usually deteriorates control system performance. Therefore, traditional IT security cannot completely provide the desired level of defense against malicious insiders and computer hackers who target NCSs.

In our proposed cyber-physical wide-area power system architecture the PMU measurement data (states) and the excitation inputs (control inputs) from the distributed controllers (VMs) are transported over a shared relatively open network thereby increasing the potential risk of security hacks by adversaries and network congestion. There are various kinds of security attacks possible, such as Denial-of-Service (DoS), desynchronization, and data injection attacks [60].

3.1 Denial-of Service Attacks

Availability of a control system refers to the ability of all components of the system being accessible. Lack of availability results in Denial-of-Service of sensor and control data. The broken red lines in the represents the DoS attack, where the adversary prevents two entities from communicating [44]. To launch a DoS attack the adversary can jam the communication channels, compromise devices and prevent them from sending data, attack the routing protocols, flood with network traffic etc. as shown by analysis of a database that tracked cyber-incidents affecting industrial control systems from 1982 to 2003 [61]. DoS is the most likely threat to control systems; therefore in this work we focus on DoS attacks, and propose two mitigation strategies to reduce its negative impacts on the proposed delay-aware optimal controller performance.
3.1.1 Security Attack Parameters

An attacker may induce DoS attacks potentially on any of the communication links connecting VM nodes between any two inter-area or intra-area nodes as shown in Fig. 2.4, and at any time instant during the transient response of the system following a small-signal disturbance. The duration of the attack can also be arbitrary. However, we assume the duration to be upper bounded, as with current intrusion detection systems (IDS)[62], DoS can be detected and mitigated through filtering and routing through alternate routes fairly quickly. We, therefore, study the performance of our proposed delay-aware LQR controller by considering three attack parameters:

1. **Network Link Location** - based on the location of actual synchronous machines in the grid, the location of the VMs assigned to represent a balancing authority in the cloud may also be geographically close or distant. The links connecting the distant nodes are more critical for DoS as they will result in more noticeable delays. Effectively there are two different groups of links possible in a wide-area networked system

   - **Inter-Area Links**: Communication links connecting VM controller nodes between two geographically far apart areas, irrespective of the physical connectivity of the corresponding generators.
   - **Intra-Area Links**: Communication links connecting VM controller nodes within a local area.

2. **Time Instant of Attack** - the time instant at which the attack is induced; this instant may be counted, for example, with respect to the settling-time of the closed-loop system due to a small perturbation in the equilibrium.
3. **Duration of Attack** - the number of data samples of the state measurements delayed or lost due to the attack, i.e., the total time of attack on a network link.

### 3.1.2 Performance Criteria

To compare the effects of various DoS attacks induced by varying the security attack parameters mentioned in 3.1.1 we need a common performance criteria measure for each attack scenario. The performance criteria should be a direct bearing towards the effectiveness of the proposed controller and stability of the closed loop system. In our case, since we have designed an optimal LQR controller the cost function $J$ from Eq. 2.74 is an obvious choice for the performance criteria.

The performance criteria we measure are

- **State Energy** ($E_s$) - The minimum quadratic energy of the states of the dynamic system.
- **Input Energy** ($E_u$) - The minimum quadratic energy of the inputs of the dynamic system.
- **Quadratic Cost Function ($J$)** - The minimum of the quadratic cost function or the objective function of the LQR controller designed.

\[
J = E_s + E_u
\]  

The objective of the LQR controller is to minimize the quadratic cost function $J$ and hence the controller performance degradation is comparatively lesser for those cases where
3.1. DENIAL-OF-SERVICE ATTACKS  
CHAPTER 3. CYBER ATTACKS AND MITIGATION

the $J$ value is lower. Higher value of $J$ indicates that the closed loop system is closer to instability. In order to have a relative scale to define the effectiveness of the controller, we normalize the performance criteria with respect to the nominal State Energy, Input Energy and Quadratic Cost Function of the dynamic system with network delays but without any DoS attack.

3.1.3 Mitigation Strategy

We propose two mitigation strategies to reduce the effect of DoS attacks on our closed-loop control system:

1. Strategy I: Skip Strategy

   In this strategy the state measurements of the machines are assumed to be zero if they are not available at the controller node within the maximum network delay threshold, $h$ seconds. The control input of $i^{th}$ machine thus calculated can be mathematically represented by,

   $$ u_i[k] = (K_0 \circ G_A)x[k] + (L_0 \circ G_A)u[k-1] $$  \hspace{1cm} (3.2)

   where $G_A$, the communication network graph of cyber-physical system under security attack, is constructed by zeroing out the entries of $G$ from Eq. 2.66, that correspond to the attacked links, $G_A = [G_A \mid G_A \mid G_A]$ is the state availability matrix of a system under cyber attack. The subscript $i$ denotes the $i^{th}$ row of the respective matrices.

2. Strategy II: Zero-order Hold

   In this strategy each VM is assumed to store the values of its assigned states, so that the states at previous instant of time are available at any sampling instant. If state
3.2. SEVERITY CLASSIFICATION

We next quantify the impact of DoS attacks on the controller performance by considering the closed-loop LQR quadratic cost function Eq. 2.74 as a function of the three random attack parameters stated above. With extensive simulation data, and using statistical tools we build a decision tree classifier to determine the conditions at which the controller performance is critical. The attack parameters are the input attributes, and the quadratic
cost is the resulting performance criteria. The attack parameters are varied with respect to a Gaussian distribution, and the data points are split into discrete bins of data as the simulation attributes and the measured performance criteria are continuous variables.

Based on the relative value of the performance criteria ($J$, $E_s$ and $E_u$) with respect to the nominal values for a system without security attack, the performance of the system is split into four classes of severity.

- **Link Location:** It is split into two discrete groups - inter-area and intra-area links.

- **Time instant:** It is split into number of separate pre-defined time instants, which are decided while designing the DoS experiment. The time instants of attack for the simulation are chosen from a normal distribution of time instant with an equal interval starting from 0.2% till 60% of the settling time of the perturbed dynamic system.

- **Duration:** It is split into the number of discrete intervals of time or number of samples. The experiments are designed in such a manner that the duration of attack is varied between a minimum and maximum number of samples with a constant interval.

The objective of severity classification of the DoS attack is to classify or identify those set of security attack parameters which has a high probability of critical performance degradation of the controller. The first step for computing the decision tree is to evaluate the mutual information (MI) between the attack parameters and resulting quadratic cost values using the Kullback entropy approach [63]. Mutual information, in essence, captures the correlation between the input attribute (attack parameters) and the output function.
3.2. SEVERITY CLASSIFICATION

CHAPTER 3. CYBER ATTACKS AND MITIGATION

(LQR energy of closed-loop system). The Kullback entropy $K(p|p^0)$ between two probability distributions $p$ and $p^0$ is given as

$$K(p|p^0) = \sum p_i \log \frac{p_i}{p^0_i}$$  \hspace{1cm} (3.4)

The Kullback entropy is the information gain when replacing an initial probability distribution $p^0$ by $p$. We consider a joint probability distribution $p(a_i, b_j)$ where $a_i$ is a bin in the security attack parameter and $b_j$ is a bin in the performance criteria. The mutual information between the attack parameter and the performance criteria is therefore given as

$$K(p|p^0) = \sum p(a_i, b_j) \log \frac{p(a_i, b_j)}{p(a_i)p(b_j)}$$  \hspace{1cm} (3.5)

The decision tree is built based on the following four steps,

1. Calculate the entropy of every security attack parameter using the simulation data set $S$.

2. Split the set $S$ into subsets using the parameter for which the mutual information gain is maximum.

3. Make a decision tree node containing that parameter.

4. Recursively perform the above steps on the subsets using other parameters.

The resulting decision tree classifier will have branches split based on a binary decision on each of the input attack parameters and the end leaf nodes are the discrete bins representing the severity of attack based on the values of security attack parameters in their respective branches.
In the following section we have illustrated the decision tree classifier by implementing the mutual information algorithm in matlab and using statistical tools available in matlab software. Finally in 5 we have made concluding remarks on benefits and advantages of building a decision tree classifier.
In this chapter, we will illustrate our proposed controller design and study the impacts of security attacks on the system using simulations. Then further we will build a decision tree classifier to identify the critical security attack parameters that might cause detrimental effects on the power system stability. For our experiments we consider

1. 4-machine 2-Area Kundur Model

2. 14- machine 4-Area Australian power grid model

The simulations are performed using MATLAB and Visual C++ programs.
4.1 Kundur Power System Model

The IEEE standard Kundur power system contains eleven buses and two areas, connected by a weak tie between bus 7 and 9. Totally two loads are applied to the system at bus 7 and 9. Two shunt capacitors are also connected to bus 7 and 9 as shown in Fig. 4.1 below. The system has the fundamental frequency 60 Hz.

The system comprises two similar areas connected by weak tie. Each area consists of two generators, each having a rating of 900MVA and 20kV. The left half of the system is identified as area 1 and the right half of the system is identified as area 2.

4.1.1 Small Signal Model

We have derived a linear third-order small signal model of the 4-machine power system model from the non-linear swing and excitation dynamic equations. The synchronous
Table 4.1 Load Flow results for Kundur power system model

<table>
<thead>
<tr>
<th>Synchronous machine</th>
<th>P [MW]</th>
<th>Q [Mvar]</th>
<th>$E_t$ [p.u]</th>
</tr>
</thead>
<tbody>
<tr>
<td>G1</td>
<td>700</td>
<td>185</td>
<td>1.03∠20.2 deg</td>
</tr>
<tr>
<td>G2</td>
<td>700</td>
<td>235</td>
<td>1.01∠10.5 deg</td>
</tr>
<tr>
<td>G3</td>
<td>719</td>
<td>176</td>
<td>1.03∠−6.8 deg</td>
</tr>
<tr>
<td>G4</td>
<td>700</td>
<td>202</td>
<td>1.01∠−17.0 deg</td>
</tr>
</tbody>
</table>

generator, load, and transmission line parameters are specified in A. The load flow analysis is performed and initial conditions of the generator buses are identified. The power flow results from [49] are shown in Table 4.1. The non-linear dynamic system from Eq. 2.1-Eq. 2.5 is linearized at the initial operation conditions. The state space model of the continuous-time system Eq. 2.65 is built in MATLAB. The frequency of data acquisition by the PMUs at each generator bus is chosen to be 20Hz and hence the sampling time of the effective discrete-time system is 0.05 seconds. The discrete-time state space model (Eq. 2.67) is derived in MATLAB using a zero-order hold.

A LQR controller is designed for this discrete time system to analyze the closed-loop response of the system. The closed loop response and the excitation inputs to the generators are shown in Fig. 4.2 and Fig. 4.3. From the below shown figure it is evident that the steady state error of the closed loop system is zero and the oscillations of the systems settle down at 14.35 seconds. It is also quite obvious that the system is stable.
4.1. KUNDUR POWER SYSTEM MODEL  

CHAPTR 4. SIMULATION AND RESULTS

4.1.2 Cyber-physical model

The cyber-physical network architecture for the 4-machine kundur model follows from Section 2.2.1. PMUs are placed at all the four generator buses and transmits state measurements at 20Hz frequency to the local VM node corresponding to the respective generator.
The VMs are connected in full graph architecture and all the VMs are interconnected with each other and they transmit the states and control input at the previous time sample to all the other VMs. The delay threshold \( (h) \) is assumed to be 0.03 seconds (i.e.) the data is considered to be lost if it does not reach a VM node within 30 ms. The control input of the cyber-physical system with network delays is calculated only after 0.03 seconds at each time sample.

The discrete-time state space model of the system with 12 states is modified into the 16-state dynamic system with delays by augmenting the control input from the previous time instant as shown in Eq. 2.73. A LQR controller as mentioned in Section 2.3 is designed. The closed-loop response and control inputs of the system with network delays is shown in Fig. 4.4 and Fig. 4.5, respectively.

![Figure 4.4 Closed loop response of the discrete-time system with network delays](image)
4.1.3 Cyber-Attack Simulation

We perform denial-of-service attack simulations on the cyber links of the cyber-physical wide-area system model derived in the above sections. The security attack simulations are performed using Visual C++ application developed based on armadillo linear algebra package. Since we have chosen a detailed third order model and running the simulation for a number of scenarios by varying the security attack parameters, the computational complexity is high and MATLAB program runs for several hours. Hence we developed a C++ based simulation which can run the exact same simulations much faster than MATLAB. The DoS scenarios are decided based on the choice of the security attack parameters mentioned in Section 3.1.1. In the 4-machine Kundur model,
4.1. KUNDRU POWER SYSTEM MODEL

CHAPTER 4. SIMULATION AND RESULTS

Table 4.2 Network Links in network architecture of IEEE Kundur 4-machine model

<table>
<thead>
<tr>
<th>Intra-Area Links</th>
<th>Inter-Area Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>G1-G2</td>
<td>G1-G3</td>
</tr>
<tr>
<td>G3-G4</td>
<td>G1-G4</td>
</tr>
<tr>
<td></td>
<td>G2-G3</td>
</tr>
<tr>
<td></td>
<td>G2-G4</td>
</tr>
</tbody>
</table>

1. **Network Link Location** - There are a total of six links interconnecting the VM nodes. The two links connecting VMs present at G1 and G2, and G3 and G4 are local intra-area links which connect the generators within an area. The other four links connecting the VMs of two generators of different areas are called the inter-area links.

2. **Time Instant of Attack** - The time instant at which the attack is induced with respect to the settling time of the system. In our simulations we have chosen a uniform distribution of time instants of attack. We have chosen 10 time instances at equal intervals starting from 0.2% to 60% of the settling time of the system with network delays.

3. **Duration of Attack** - It is the number of time samples lost due to the DoS attack. In our simulation we vary the duration between 20 samples to 200 samples and at equal intervals. We perform the simulation for ten different duration.

We have run the simulations by varying the security attack parameters as mentioned above and measured the objective cost function $J$ for each set of security parameters. We calculate the percentage difference in measured $J$ with respect to the minimum $J$ of the
nominal power system with network delays.

$$J_{\text{percent}} = \frac{J_{\text{attack}}}{J_{\text{nominal}}} \times 100$$ \hspace{1cm} (4.1)

In Fig. 4.6, we compare the phase angle plots at each generator bus for a system with DoS attack induced at 0.6 seconds and for a duration of 20 samples (1 second), to a system without DoS. As shown in the legend, the green line represents the network delayed system with no security attack, and the blue and red lines represent the systems with strategy I and strategy II implemented to mitigate the DoS attack.

Figure 4.6 Kundur Model - Phase angles plots at all generator buses for systems with and without DoS Attack.
In what follows, we have included the plots of the percentage variation in $J$ with respect to each cyber link of the 4-machine 2-area kundur power system. For each chosen link which has been attacked we vary the time instant of attack based on the settling time of the nominal network dynamic system and also the duration of attack. The plots are color coded 3D plots, where the x-axis is the time instant of attack, y-axis is the duration of attack and z-axis is the percentage variation in the measured value of the cost function $J$.

### 4.1.3.1 Intra-Area Links

The Fig. 4.7 and Fig. 4.8 represent the percentage variation in $J$ from nominal value of $J$ for a DoS attack executed at the intra-area link connecting generators $G_1$ and $G_2$ of Area 1. Fig. 4.9 and Fig. 4.10 represent the same for a DoS attack simulated at the intra-area link connecting generators $G_3$ and $G_4$ of Area 2.

![Figure 4.7 Kundur Model - Variation of $J$ when the security attack is between link connecting generators G1-G2 and strategy I is implemented.](image)
4.1. KUNDUR POWER SYSTEM MODEL  

CHAPTER 4. SIMULATION AND RESULTS

Figure 4.8 Kundur Model - Variation of $J$ when the security attack is between link connecting generators G1-G2 and strategy II is implemented.

4.1.3.2 Inter-Area Links

The 3-D plots shown below represent the variation in the LQR objective cost function $J$ with respect to the nominal value of the cost function for a network dynamic system in the absence of DoS. The links considered are inter-area links, i.e., links connecting generators from one area to another.

From the above plots it can be observed that the variation in $J$ is greater when the time instant of attack is closer to the initiation of perturbation or fault in the system. It can also be seen that the performance degrades as the duration of attack is increased. Finally, a comparing the trends between inter-area links and intra-area links it can be seen that the ill-effects on the system is greater when the attacks are between inter-area links.
4.1. KUNDUR POWER SYSTEM MODEL

CHAPTER 4. SIMULATION AND RESULTS

Figure 4.9 Kundur Model - Variation of $J$ when the security attack is between link connecting generators G3-G4 and strategy I is implemented.

Figure 4.10 Kundur Model - Variation of $J$ when the security attack is between link connecting generators G3-G4 and strategy II is implemented.
Figure 4.11 Kundur Model - Variation of $J$ when the security attack is between link connecting generators G1-G3 and strategy I is implemented.

Figure 4.12 Kundur Model - Variation of $J$ when the security attack is between link connecting generators G1-G3 and strategy II is implemented.
Figure 4.13 Kundur Model - Variation of $J$ when the security attack is between link connecting generators G1-G4 and strategy I is implemented.

Figure 4.14 Kundur Model - Variation of $J$ when the security attack is between link connecting generators G1-G4 and strategy II is implemented.
4.1. KUNDUR POWER SYSTEM MODEL  

CHAPTER 4. SIMULATION AND RESULTS

Figure 4.15 Kundur Model - Variation of $J$ when the security attack is between link connecting generators G2-G3 and strategy I is implemented.

Figure 4.16 Kundur Model - Variation of $J$ when the security attack is between link connecting generators G2-G3 and strategy II is implemented.
Figure 4.17 Kundur Model - Variation of $J$ when the security attack is between link connecting generators G2-G4 and strategy I is implemented.

Figure 4.18 Kundur Model - Variation of $J$ when the security attack is between link connecting generators G2-G4 and strategy II is implemented.
4.2 Australian power system model

The Simplified 14-generator, 50 Hz system is shown in Fig. 4.19. These machines are divided into 4 areas and hence 3 inter-area modes, as well as 10 local-area modes. The
4.2. AUSTRALIAN POWER SYSTEM MODEL  
CHAPTER 4. SIMULATION AND RESULTS

generators in each area, denoted by red dots, are: $G_1G_5$ in Area 1, $G_6G_7$ in Area 2, $G_8G_{11}$ in Area 3, and $G_{12}G_{14}$ in Area 4.

4.2.1 Small Signal Model

We have derived a linear third-order small signal model of the 14-machine power system model from the non-linear swing and excitation dynamic equations. The synchronous generator, load, and transmission line parameters are specified in A. The load flow analysis is performed and initial conditions of the generator buses are identified.

The non-linear dynamic system from Eq. 2.1-Eq. 2.5 is linearized at the initial operation conditions identified by the load flow analysis. The state space model of the continuous-time system Eq. 2.65 is built in MATLAB. The frequency of data acquisition by the PMUs at each generator bus is chosen to be 20Hz and hence the sampling time of the effective discrete-time system is 0.05 seconds. The discrete-time state space model (Eq. 2.67) is derived in MATLAB using a zero-order hold.

A LQR controller is designed for this discrete time system to analyze the closed-loop response of the system. The closed loop response and the excitation inputs to the generators are shown in Fig. 4.20 and Fig. 4.21. From the below shown figure it is evident that the steady state error of the closed loop system is zero and the oscillations of the systems settle down at 22.6 seconds. It is also obvious that the closed loop system is stable.

4.2.2 Cyber-physical model

The cyber-physical network architecture for the 14-machine kundur model follows from Section 2.2.1. PMUs are placed at all the fourteen generator buses and transmits state
4.2. AUSTRALIAN POWER SYSTEM MODEL  

CHAPTER 4. SIMULATION AND RESULTS

Figure 4.20 Closed loop response of the discrete-time system

Figure 4.21 Excitation control inputs to the machines of the discrete-time system

measurements at 20 Hz frequency to the local VM node corresponding to the respective generator. The VMs are connected in full graph architecture and all the VMs are interconnected with each other and they transmit the states and control input at the previous time sample to all the other VMs. The delay threshold \( h \) is assumed to be 0.03 seconds (i.e.) the data is considered to be lost if it does not reach a VM node within 30 ms. The control input
of the cyber-physical system with network delays is calculated only after 0.03 seconds at each time sample.

The discrete-time state space model of the system with 42 states is modified into the 56-states dynamic system with delays by augmenting the control input from the previous time instant as shown in Eq. 2.73. A LQR controller as mentioned in Section 2.3 is designed. The closed-loop response and control inputs of the system with network delays is shown in Fig. 4.22 and Fig. 4.23, respectively.

![Figure 4.22 Closed loop response of the discrete-time system with network delays](image)

### 4.2.3 Cyber-Attack Simulation

We perform denial-of-service attack simulations on the cyber links of the cyber-physical wide-area system model derived in the above sections. The security attack simulations are performed using Visual C++ application developed based on armadillo linear algebra...
4.2. AUSTRALIAN POWER SYSTEM MODEL  CHAPTER 4. SIMULATION AND RESULTS

Figure 4.23 Excitation control inputs to the machines of the discrete-time system with network delays

package. Since we have chosen a detailed third order model and running the simulation for a number of scenarios by varying the security attack parameters. The DoS scenarios are decided based on the choice of the security attack parameters mentioned in 3.1.1. In the 14-machine Australian power system model,

1. **Network Link Location** - There are a total of $\binom{14}{2} = 91$ links interconnecting the VM nodes, which includes 20 intra-area links and 71 Inter-Area links. The intra-area links connect the VM nodes within a local region whereas the inter-area links connect the VM nodes of two areas.

2. **Time Instant of Attack** - The time instant at which the attack is induced with respect to the settling time of the system. In our simulations we have chosen a uniform distribution of time instants of attack. We have chosen 10 time instances at equal intervals starting from 0.2% to 60% of the settling time of the system with network delays.
3. **Duration of Attack** - It is the number of time samples lost due to the DoS attack. In our simulation we vary the duration between 20 samples to 200 samples and at equal intervals. We perform the simulation for ten different duration.

We have run the simulations by varying the security attack parameters as mentioned above and measured the objective cost function $J$ for each set of security parameters. We calculate the percentage difference in measured $J$ with respect to the minimum $J$ of the nominal power system with network delays.

In Fig. 4.24, we compare the phase angle plots at each generator bus for a system with DoS attack induced at 0.6 seconds and for a duration of 100 samples (5 seconds), to a system without DoS. Both the systems are network dynamic systems with a nominal network delay of 0.03 seconds.

In what follows, we have included the plots of the percentage variation in $J$ with respect to communication links of the 14-machine 4-area Australian power system. For each chosen link which has been attacked we vary the time instant of attack based on the settling time of the nominal network dynamic system and also the duration of attack. The plots are color coded 3D plots, where the x-axis is the time instant of attack, y-axis is the duration of attack and z-axis is the percentage variation in the measured value of the cost function $J$.

### 4.2.3.1 Intra-Area Links

The Fig. 4.25 and Fig. 4.26 represent the percentage variation in $J$ from nominal value of $J$ for a DoS attack executed at the intra-area link connecting generators $G9$ and $G10$ of Area 3.
Figure 4.24 Australian Power System - Phase angles plots at all generator buses for system with and without DoS Attack.

4.2.3.2 Inter-Area Links

The 3-D plots shown below represent the variation in the LQR objective cost function $J$ with respect to the nominal value of the cost function for a network dynamic system in the absence of DoS. The links considered are inter-area links, i.e., links connecting generators from one area to another.

From the above plots it can be observed that the variation in $J$ is greater when the time instant of attack is closer to the initiation of perturbation or fault in the system and as the duration of attack is longer. Similar to the 4-machine kundur model it can be noted that the
4.2. AUSTRALIAN POWER SYSTEM MODEL  CHAPTER 4. SIMULATION AND RESULTS

Figure 4.25 Australian power grid - Variation of \( J \) when the security attack is between link connecting generators G9-G10 and strategy I is implemented.

Performance degradation effects on inter-area links are more than that on the intra area links.
Figure 4.26 Australian power grid - Variation of $J$ when the security attack is between link connecting generators G9-G10 and strategy II is implemented.

Figure 4.27 Australian power grid - Variation of $J$ when the security attack is between link connecting generators G1-G11 and strategy I is implemented.
4.2. AUSTRALIAN POWER SYSTEM MODEL  CHAPTER 4. SIMULATION AND RESULTS

Figure 4.28 Australian power grid - Variation of $J$ when the security attack is between link connecting generators G1-G11 and strategy II is implemented.

Figure 4.29 Australian power grid - Variation of $J$ when the security attack is between link connecting generators G2-G7 and strategy I is implemented.
4.2. **AUSTRALIAN POWER SYSTEM MODEL**  

CHAPTER 4. **SIMULATION AND RESULTS**

Figure 4.30 Australian power grid - Variation of $J$ when the security attack is between link connecting generators G2-G7 and strategy II is implemented.
4.3 Severity Classification

From the simulation data collected for a two area four machine kundur system, we have built a decision tree classifier based on the kullback entropy technique as mentioned in Section 3.2. The decision tree classifies the security attacks into four categories based on the severity as shown in the Table 4.3. Two separate decision trees are built for each strategy. The data is split into discrete bins, and $J$ is classified into four critical categories. $J_{14}$ indicates the bin with highest changes in nominal value of $J$ (without attack). The triangles represent the decision points with respect to the three attack parameters, each triangle has two downward branches depending on a binary decision. The circles represent the discrete bins of $J$.

4.3.1 Kundur Power System Model

The classification tree in Fig. 4.31, the $J$ values measured for various security attack scenarios mentioned in the above sections are classified into four categories for a 4-machine,2-area kundur model with strategy I implemented to mitigate the DoS attack. $J_{11}$ being the safest

Table 4.3 Classification of $J$ into discrete bins

<table>
<thead>
<tr>
<th>Strategy I</th>
<th>Strategy II</th>
<th>% variation in $J$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$J_{11}$</td>
<td>$J_{21}$</td>
<td>0-15</td>
</tr>
<tr>
<td>$J_{12}$</td>
<td>$J_{22}$</td>
<td>15-35</td>
</tr>
<tr>
<td>$J_{13}$</td>
<td>$J_{23}$</td>
<td>35-60</td>
</tr>
<tr>
<td>$J_{14}$</td>
<td>$J_{24}$</td>
<td>$\geq$60</td>
</tr>
</tbody>
</table>
and $J_{14}$ is the most critical set of values of $J$, i.e. the performance degradation is high. The discrete bins are identified in Table 4.3.

From Fig. 4.31, the severity classification tree for Kundur power system model when strategy I is implemented, it can be seen that in our simulation the most critical values of $J$ in bin $J_{14}$ are attained when links in A2 (Inter-area links) are attacked at any time instant less than 0.975 seconds from the time of disturbance, and for a duration of greater than 30 samples. It can also be observed that in most cases if the attack is launched after 1.45 seconds, then $J$ lies in the bins $J_{11}$ or $J_{12}$, i.e. the severity of the attack is less. The tree also shows the relative dependence of the three attack parameters. For example, $J$ lies in bin $J_{13}$ (reasonably critical) when the duration of attack is less than 30 samples, time of attack is at any instant less than 0.975 seconds and at links in A2; and it also lies in the same bin for duration more than 30 samples when the time of attack is greater than 0.525 seconds for the links in A1.

The Fig. 4.32 represents the severity classification tree for the 4-machine 2-Area Kundur power system model when strategy II is implemented to mitigate the DoS attacks. From the classification tree it is evident that the most critical values of $J$, i.e. in bin $J_{24}$, are observed when the DoS attack is launched at any time instant less than 1.05 seconds and for a duration more than 30 samples. It is also observed that for most cases where the DoS attack occurs after 4.75 seconds from the instant of disturbance the value of $J$ lies in the less critical bins $J_{11}$ and $J_{12}$. It is also noted that the values of $J$ in bin $J_{23}$ are more probable when the links in A2 (Inter-area links) area attacked.
4.3. SEVERITY CLASSIFICATION

CHAPTER 4. SIMULATION AND RESULTS

Figure 4.31 Kundur-Model - Strategy I - Decision tree classifier. Classifies the cost function of strategy I into 4 classes based on the severity

Figure 4.32 Kundur Model - Strategy II - Decision tree classifier. Classifies the cost function of strategy II into 4 classes based on the severity
4.3.2 Australian Power System Model

From Fig. 4.31, the severity classification tree for Australian power system model when strategy I is implemented, it can be seen that the decision tree predicts critical values of $J$ in bin $J_{14}$ are attained when links in A2 (Inter-area links) are attacked at any time instant less than 1.05 seconds from the time of disturbance, and for a duration of greater than 90 samples, with the data from our simulation. It can also be observed that in most cases if the attack is launched after 2.925 seconds, then $J$ lies in the bins $J_{11}$, i.e. the severity of the attack is less.

![Decision tree classifier](image)

Figure 4.33 Australian Power System - Strategy I - Decision tree classifier. Classifies the cost function of strategy 1 into 4 classes based on the severity

Fig. 4.34 represents the severity classification tree for the Australian power system model.
when strategy II is implemented to mitigate the DoS attack. The most critical values of $J$ in bin $J24$ are observed when the attack is induced within 1.05 seconds of disturbance and for a duration greater than 70 samples. The same occurs for a duration less than 70 samples but greater than 50 samples and attacked link is in A1 (Intra-area links). Similarly in most cases where the attack is induced after 3.85 seconds from the time of disturbance, the value of $J$ lies in bins $J11$ or $J12$, i.e. the severity of the attack is less.

Figure 4.34 Australian Power System - Strategy II - Decision tree classifier. Classifies the cost function of strategy 1 into 4 classes based on the severity
The Cyber-Physical system network security research conducted in this work includes the analysis of severity of the security threats based on the chosen security attack parameters. In this work, we have proposed two mitigation strategies to reduce the ill-effects of a cyber attack on a wide-area control by modifying the optimal controller design. Then we have designed decision tree classifier to classify the severity of the denial-of-service (DoS) attacks for both the proposed mitigation strategies.

In this work, we illustrated our experiments and results by performing MATLAB and
C++ simulations of two standard IEEE wide-area power system models:

- Two-Area Four-Machine Kundur Model
- Four-Area Fourteen-Machine Australian power grid model

For both the models, we first design a linear quadratic regulator (LQR) controller for the linearized small signal discrete system considering that the state measurements of all the machines are available through PMU measurements at each generator bus. Further we have defined the network architecture of the cyber physical system and derived the models taking into account the delays in the network. We designed a delay-aware LQR controller for the network dynamic system with delays. The closed loop response and designed excitation control inputs for both the models are presented in Chapter 4.

With the developed controllers, we designed cyber security attack scenarios and performed denial-of-service attack simulations in C++ by varying the security attack parameters. The performance characteristic of the controller for each scenario is measured by evaluating the LQR objective cost function ($J$). The measured $J$ are then classified into four categories based on severity. Finally we designed a decision tree classifier based on the kullback entropy approach , following Section 3.2.

The 3-D surface plots of variation in $J$ for a system with security attack from a nominal value of $J$ indicates that the effect of DoS attack on the system is greater or the performance of the controller is worse, when the time instant of attack is closer to the time of perturbation in the system and when the duration of attack is high. It is also observed that the attacks on inter-area links, the links connecting VMs of two different areas, have a comparatively greater impact than intra-area links (links connecting VMs within a local area).
In both of the wide-area systems we have simulated in this experiment, it is observed that the strategy II, where the states of previous time instant are used during a DoS attack, has a better performance compared to that of Strategy I, where the missing states are skipped. The only drawback in implementation of strategy II over strategy I is that, the former requires memory to store previous state measurements and it would be a large amount of space on each VM when applied on a large scale wide-area network.

Finally, the severity classification tree are built for each strategy based on the simulation experiments. This result can be used at the design phase of the cyber-physical architecture to strengthen the security and improve the bandwidth of the critical links identified by the decision tree. The decision tree can also be utilized to predict the performance of the controller for any set of security attack parameters chosen. Therefore, the research work presented in this thesis can be performed for any known power system model and will be helpful in identifying a secure network architecture by conducting simulation studies during the design phase.

5.1 Future Work

This study provides a basic framework for analysis of denial-of-service attacks on a cyber physical wide-area power system based on software simulations. This can be further expanded in following ways

- *Real Time Simulations* - A more accurate study of behavior of the power system and the communication network can be achieved by running real-time hardware-in-loop simulations using the power system simulators such as RTDS (Real Time
Digital Simulator) and OPAL-RT. The network dynamics can be simulated by taking advantage of network simulators like Exo-GENI or DETER network testbeds.

• **Performance Measures** - Alternative metrics such as frequency-domain properties including closed-loop gain margins, or condition number of closed-loop state matrix, etc. all of which quantify the impact of attacks on the system performance can be used to identify the severity of the security attack and construct the decision tree.

• **Different Security Attacks** - Man-in-middle attack, data intrusion and data corruption are few other kinds of security attacks that are possible in a communication system. The effects of these attacks on the system can be studied.

• **More Complex Control Strategies** - Instead of Optimal control techniques, complex real time control strategies can be implemented. To name a few Adaptive control, robust control and model predictive control can be suitable for this application. State estimation based on kalman filters can be used to estimate the missing states and the trade off between performance improvement and computational complexity can be studied.


[56] Conti, J. “The day the samba stopped [power blackouts]”. Engineering & Technology 5.4 (2010), pp. 46–47.


APPENDIX
APPENDIX

A

MODEL PARAMETERS

A.1 IEEE Standard Kundur Power System Model

Kundur’s Two-Area Four-Machine system consisting of two fully symmetrical areas linked together by two 220 km, 230 kV transmission lines is considered as a first case study in this research. This power system typically is used to study the low frequency electromechanical oscillations of a large interconnected system. All the generators in the model are considered to be similar and the generator parameters are given by
A.2. SIMPLIFIED 14-GENERATOR AUSTRALIAN POWER SYSTEM

Table A.1 Generator Parameters for the 4-machine 2-Area Kundur Model

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R_a$</td>
<td>0.0025</td>
</tr>
<tr>
<td>$X_d$</td>
<td>1.8</td>
</tr>
<tr>
<td>$X_q$</td>
<td>1.7</td>
</tr>
<tr>
<td>$X_1$</td>
<td>0.2</td>
</tr>
<tr>
<td>$X'_d$</td>
<td>0.25</td>
</tr>
<tr>
<td>$X'_q$</td>
<td>0.25</td>
</tr>
<tr>
<td>$T_{do}$</td>
<td>8.0s</td>
</tr>
<tr>
<td>$T_{d0}$</td>
<td>0.40s</td>
</tr>
<tr>
<td>$T_{d'}$</td>
<td>0.03s</td>
</tr>
<tr>
<td>$T_{d''}$</td>
<td>0.05s</td>
</tr>
<tr>
<td>$H$</td>
<td>6.5</td>
</tr>
<tr>
<td>RATING</td>
<td>900 MVA</td>
</tr>
</tbody>
</table>

A.2 Simplified 14-generator Australian Power System

Table A.2 Generator Parameters for the 14-machine simplified Australian Power Grid

| Generator | Bus | Order | Rating MVA | No. of Units | H-MWs/MVA | Xa (pu) | Xd (pu) | Xq (pu) | Xd' (pu) | Xd'' (pu) | Xd" (pu) | Td0 (s) | Td0' (s) | Td0" (s) | Xq' (pu) | Tq0' (s) | Xq" (pu) | Tq0" (s) | Tq0" (s) |
|-----------|-----|-------|------------|--------------|-----------|---------|--------|--------|---------|----------|----------|---------|---------|----------|---------|---------|---------|---------|---------|---------|
| HP1S      | 101 | 5     | 333.3      | 12           | 3.60      | 0.14    | 1.10   | 0.65   | 0.25    | 8.50     | 0.25     | 0.050   | -       | -       | -       | 0.25    | 0.25    | 0.20    | 0.20    | 0.050   |
| BP1S      | 201 | 6     | 666.7      | 6            | 3.20      | 0.20    | 1.80   | 1.75   | 0.30    | 5.00     | 0.20     | 0.040   | 0.70    | 0.30    | 0.21    | 0.080   | 0.080   | 0.080   |
| EP1S      | 202 | 6     | 555.6      | 5            | 2.80      | 0.17    | 2.20   | 2.10   | 0.30    | 5.00     | 0.20     | 0.040   | 0.50    | 0.20    | 0.040   | 0.040   | 0.040   |
| MP1S      | 204 | 6     | 666.7      | 6            | 3.20      | 0.20    | 1.80   | 1.75   | 0.30    | 5.00     | 0.20     | 0.040   | 0.70    | 0.30    | 0.21    | 0.080   | 0.080   |
| VP1S      | 203 | 6     | 555.6      | 4            | 2.60      | 0.20    | 2.30   | 1.70   | 0.30    | 5.00     | 0.25     | 0.030   | 0.40    | 0.25    | 0.25    | 0.25    | 0.25    |
| LP1S      | 301 | 6     | 666.7      | 4            | 2.80      | 0.20    | 2.70   | 1.50   | 0.30    | 7.00     | 0.25     | 0.040   | 0.85    | 0.85    | 0.25    | 0.120   |
| TP1S      | 302 | 5     | 444.4      | 4            | 3.50      | 0.15    | 2.00   | 1.80   | 0.25    | 7.50     | 0.20     | 0.040   | -       | -       | 0.20    | 0.25    |
| CP1S      | 402 | 6     | 333.3      | 3            | 3.00      | 0.20    | 1.90   | 1.80   | 0.30    | 6.50     | 0.26     | 0.035   | 0.55    | 1.40    | 0.26    | 0.040   |
| GP1S      | 404 | 6     | 333.3      | 6            | 4.00      | 0.20    | 2.20   | 1.40   | 0.32    | 9.00     | 0.24     | 0.040   | 0.75    | 1.40    | 0.24    | 0.130   |
| SP1S      | 403 | 6     | 444.4      | 4            | 2.60      | 0.20    | 2.30   | 1.70   | 0.30    | 5.00     | 0.25     | 0.030   | 0.40    | 2.00    | 0.25    | 0.25    | 0.25    |
| TP1S      | 401 | 6     | 444.4      | 4            | 2.60      | 0.20    | 2.30   | 1.70   | 0.30    | 5.00     | 0.25     | 0.030   | 0.40    | 2.00    | 0.25    | 0.25    | 0.25    |
| NP1S      | 501 | 6     | 333.3      | 2            | 3.50      | 0.15    | 2.20   | 1.70   | 0.30    | 7.50     | 0.24     | 0.025   | 0.80    | 1.50    | 0.24    | 0.100   |
| TP1S      | 502 | 6     | 250.0      | 4            | 4.00      | 0.20    | 2.00   | 1.50   | 0.30    | 7.50     | 0.22     | 0.040   | 0.80    | 3.00    | 0.22    | 0.200   |
| PP1S      | 503 | 6     | 166.7      | 6            | 7.50      | 0.15    | 2.30   | 2.00   | 0.25    | 5.00     | 0.17     | 0.022   | 0.35    | 1.00    | 0.17    | 0.035   |

88