A Biologically Inspired Hierarchical Cyber-Physical Integrated Security Analysis Framework for Smart Grids

by

Jin Kocsis

A thesis submitted in conformity with the requirements for the degree of Doctor of Philosophy Graduate Department of Electrical and Computer Engineering University of Toronto

© Copyright 2014 by Jin Kocsis
Abstract

A Biologically Inspired Hierarchical Cyber-Physical Integrated Security Analysis Framework for Smart Grids

Jin Kocsis
Doctor of Philosophy
Graduate Department of Electrical and Computer Engineering
University of Toronto
2014

The last few years have witnessed the radical transformation in structure and functionality of electrical energy systems. Such systems were traditionally executed in the physical world and are now also cyber-enabled. This cyber-enabled energy system, called smart grid, can be envisioned as the marriage of information technology with the electricity network. While its increased dependence on cyber infrastructure aims to enable greater reliability, efficiency and capacity of power delivery, this reliance also creates a host of unfamiliar vulnerabilities. Due to the highly integrated and connected nature of smart grids, it is important to account for their salient cyber-physical coupling when making critical design decisions and identifying solutions to promote security.

In this dissertation, we present a biologically-inspired cyber-physical integrated security analysis framework for maintaining smart grid stability under various forms of physical and cyber attacks. Through this security analysis framework, we demonstrate real-time cyber-physical integrated control and communication strategies using ”wisely”-placed Phasor Measurement Units (PMUs) and energy storages. Our research has evolved in three stages. We first propose a cyber-physical multi-agent dynamical systems paradigm to model the cyber-physical interactions in smart grids, in which each agent is modeled as having dynamics that synergistically describe physical and information couplings with neighboring agents. Inspired by the analogy between the flocking rules and the smart grid stability requirements, we develop a flocking-based scheme to formulate the cyber-physical integrated action for each agent. In the second stage, we extend the multi-agent dynamical systems paradigm to a two-tier hier-
archival framework which reduces information acquisition by leveraging physical couplings between the agents and applying cyber controls selectively on critical agents. In the context of the hierarchical framework, we propose a witness-based security protocol for identifying and mitigating information corruption on the critical agents. In the third stage, we develop an intelligent multicast routing strategy for timely synchronous data delivery in smart grids, called Goal-Seeking Obstacle and Collision Evasion (GOALiE), which is resilient to network congestion and Denial-of-Service (DoS) attacks.
Dedication

This thesis is dedicated to
my parents, Zhenguang Wei and Xiuqin Jia,
my husband, Terry Kocsis,
for their endless love, support, and encouragements.
Acknowledgements

First and foremost, I would like to extend my sincere regards towards Professor Deepa Kundur. Throughout my PhD studies, Professor Deepa Kundur has always been a wonderful supervisor and an exceptional mentor, from whom I learned lessons and received invaluable assistance. As a supervisor, she granted me the necessary freedom and opportunity to follow my desired research goals. She has been both the best supporter, and the critic of my ideas. Above all, Professor Deepa Kundur offered me her kind friendship, which I believe, is crucial for an international student starting her academic life far away from home. I was very lucky to have had these privileges.

Next, I would like to thank the members of the defense committee, Professors Reza Iravani, Dimitrios Hatzinakos, Konstantinos N. Plataniotis, Josh Taylor, Jan Spelt, and Jelena Misic. The comments and feedback I received from them lead to significant improvements in the quality of the thesis, both in content and presentation. I would also like to thank Professor Karen Butler-Purry in Texas A&M University for providing valuable and professional expertise as well as research equipments which greatly help me to improve my research.

I thank all my friends and colleagues from the Edwards S. Rogers Sr. Department of Electrical and Computer Engineering at the University of Toronto and Department of Electrical and Computer Engineering at the Texas A&M University, including, Xianyong Feng, Salman Mashayekh, Bo Chen, Saranya Parthasarathy, Dongchan Lee, Lili Zhang, Liu Shan, Eman Hammad, Abdallah Farraj, and many others who made the last few years a wonderful experience. I was privileged to know every single one of them. Especially, I would like to thank my good friends, Dr. Salman Mashayekh and Dr. Xianyong Feng, for their insightful feedback on parts of my research work. I wish all my friends eminent success in all their endeavors.

Finally, my deepest love and respect goes to my wonderful husband, Terry Kocsis, for all the efforts and sacrifices he made in the last few years, many of them I vividly remember, and perhaps many others that might have gone unnoticed. I was blessed with his presence, companionship, and emotional support. This is truly something I could not have attained anywhere else, at any other time, or in any other way.
Contents

1 Introduction .................................................. 1
   1.1 Background .............................................. 1
      1.1.1 Smart Grid Visions ............................... 2
      1.1.2 Security Challenges and Fundamental Questions .......... 4
   1.2 Literature Review ..................................... 6
   1.3 Problem Statement and Thesis Objectives .................. 7
   1.4 Methodology .......................................... 8
   1.5 Dissertation Outline .................................. 11

2 Flocking-Based Cyber-Physical Dynamical Systems Paradigm ...... 14
   2.1 Introduction ........................................... 14
   2.2 Dynamic Multi-Agent System Framework for Cyber-Physical Integration Modeling ..................................... 15
      2.2.1 Smart Grid Stability ................................ 15
         2.2.1.1 Rotor Angle Stability ........................ 15
         2.2.1.2 Frequency Stability ........................... 16
         2.2.1.3 Definition of Smart Grid Stability ............ 17
      2.2.2 Graph-Theoretic Dynamical Modeling for Cyber-Physical Integration ......................................... 17
         2.2.2.1 Power System Topology Reduction Analysis .... 17
         2.2.2.2 Dynamical Description ........................... 18
         2.2.2.3 Cyber-Physical Integration Framework and Dynamical Description ....................................... 19
   2.3 Flocking-Based Cyber-Physical Control Protocol Design .......... 23
      2.3.1 Flocking Theory and Formation Control ............... 23
      2.3.2 Cyber-Physical Control Protocol Design by Analogy to Flocking ............................................. 24
      2.3.3 Design by Analogy to Flocking ........................ 26
         2.3.3.1 Potential Energy Function ........................ 26
         2.3.3.2 Cyber Control Matrix B ........................... 27
2.3.3.3 Cyber Control Matrix $G$ ........................................... 27
2.3.3.4 Linear Navigation .................................................. 29
2.3.3.5 Control Signal Design ............................................ 29
2.3.4 Stability Analysis of the Proposed Control Protocol ............. 30

2.4 Robustness Analysis with the Communication Delay ............... 31
2.4.1 Communication Delay in Wide Area Power Systems .......... 31
2.4.2 Delay Analysis .......................................................... 32

2.5 Simulations and Performance Assessment .......................... 35
2.5.1 Case Study I ............................................................... 35
2.5.2 Case Study II ............................................................. 39

2.6 Conclusions ................................................................. 44

3 Two-Tier Hierarchical Cyber-Physical Security Framework ....... 45
3.1 Introduction ................................................................. 45
3.2 Two-Tier Hierarchical Cyber-Physical Control Protocol ......... 46
3.2.1 Hierarchical Cyber-Physical Dynamics .......................... 46
3.2.2 Hierarchical Control Protocol Design by Analogy to Flocking .................................................. 47
3.2.2.1 Dynamic Description of Cyber-Physical Integration .... 47
3.2.2.2 Hierarchical Cyber-Physical Dynamics ................... 49
3.2.2.3 Design by Analogy to Flocking ............................... 50
3.2.3 Hierarchical Control Protocol Stability Analysis ................ 52

3.3 Multi-Flock-Based Timely Coherency Generator Identification Method .... 54
3.3.1 Literature Review .......................................................... 54
3.3.2 Problem Setting .......................................................... 55
3.3.3 Multi-Flock-Based Generator Coherency Identification ....... 57
3.3.3.1 Multi-Flock Modeling .............................................. 58
3.3.3.2 Coherent Generator Identification ............................ 61
3.3.4 Case Studies ............................................................... 62
3.3.4.1 Ideal Environment .................................................. 64
3.3.4.2 Measurement Environment with White Noise ............ 69
3.3.4.3 Measurement Environment with False Data Injection .... 70
3.3.5 Discussion ................................................................. 71

3.4 Witness-Based Security Protocol for Information Corruption Mitigation .... 72
3.4.1 Literature Review .......................................................... 72
3.4.2 Problem Setting .......................................................... 72
3.4.3 Witness-Based Verification and Estimation Protocol ........... 73
3.4.4 Discussion .................................................. 76

3.5 Simulations and Performance Assessment ........................................... 76
  3.5.1 Ideal Environment ............................................. 77
    3.5.1.1 Case I .................................................. 77
    3.5.1.2 Case II .................................................. 80
  3.5.2 Environment With Practical Constraints of Energy Storage .............. 83
  3.5.3 Environment With Communication Delay ...................................... 84
    3.5.3.1 Fault on Line 14 − 15 .................................. 86
    3.5.3.2 Fault on Line 17 − 27 .................................. 88
  3.5.4 Environment With PMU Data Corruption ...................................... 89
    3.5.4.1 Random Attack .......................................... 89
    3.5.4.2 Collusion Attack ........................................ 91

3.6 Conclusions .......................................................... 93

4 GOAliE: A Resilient Multicast Routing Approach in Smart Grids ............... 95
  4.1 Introduction ....................................................... 95
  4.2 Problem Setting .................................................... 96
    4.2.1 Hierarchical Structure ...................................... 97
    4.2.2 Flocking for Routing ....................................... 98
  4.3 Goal-Seeking Obstacle and Collision Evasion (GOAliE) for Multi-Cast Smart
      Grid Routing .................................................... 99
    4.3.1 GOALIE Multi-hop Routing .................................. 100
      4.3.1.1 Goal Seeking Constraint ................................ 101
      4.3.1.2 Obstacle Evasion ....................................... 102
      4.3.1.3 Next Hop Selection ..................................... 102
      4.3.1.4 Collision Avoidance .................................... 102
    4.3.2 GOAliE Multicast Routing .................................... 104
      4.3.2.1 \( \zeta_{vw} \geq \zeta_{th} \) .................................. 105
      4.3.2.2 \( \zeta_{vw} < \zeta_{th} \) .................................. 105
      4.3.2.3 Multicast Dynamics and Decision-Making ............... 106
  4.4 Simulations and Performance Assessment ......................................... 107
    4.4.1 Case Study I ................................................. 108
    4.4.2 Case Study II .............................................. 114
  4.5 Conclusions .......................................................... 117
# List of Tables

2.1 Generator Parameters for WECC 3-Generator Power System .......................... 35

3.1 Neighboring Flockmate Relationships ....................................................... 59
3.2 Flockmate Dynamics .................................................................................. 63
3.3 Main Variables Used in Proposed Approach ................................................ 64
3.5 Parameters Used in Proposed Approach ....................................................... 65
3.6 Phase Angle Comparison Results (degree) .................................................... 66
3.7 Proposed Cyber-Physical Verification Scheme .............................................. 74
3.8 Proposed Cyber-Physical Estimation Scheme .............................................. 75
3.9 Comparison Between Performances of Non-Hierarchical and Hierarchical Frameworks ......................................................... 88

B.1 Spectral Matrix-Based Agent Coherency Identification Method ................... 124
B.2 Differences Between Our Test System and IEEE 14-Bus System ................. 124
B.3 Generator Parameters ............................................................. 125
List of Figures

1.1 (a) An example of smart grid, (b) Integration of power flow and communication flow in different smart grid domains [2]. .................................................. 3
1.2 Conceptual reference diagram for smart grid communication networks [2]...... 4
1.3 Methodology overview: tool-sets consisting of graph theory, dynamical-system formulation, and flocking rules. .................................................. 9
1.4 Dissertation Outline. ........................................................................... 11

2.1 Power system stability categories [3]. .................................................... 16
2.2 Kron-reduction Analysis in WECC 9-Bus System. ................................. 19
2.3 Proposed multi-agent dynamic system model. ....................................... 20
2.4 Proposed cyber-physical multi-agent dynamic system framework for the WECC 3-Generator Power System. .................................................. 22
2.5 WECC 3-Generator power system. ......................................................... 35
2.6 (a) The normalized frequencies and (b) the rotor phase angle differences versus time without control. .................................................. 36
2.7 (a) The normalized frequencies and (b) the rotor phase angle differences versus time with flocking-based control. .................................. 36
2.8 Power transmission $P_u$ between the generators and the fast-acting ESSs in the presence of our proposed protocol. ................................. 37
2.9 The block diagram of governor control system. ..................................... 37
2.10 (a) The normalized frequencies and (b) the rotor phase angle differences versus time without considering the dynamics of governor control system. .... 38
2.11 (a) The normalized frequencies and (b) the rotor phase angle differences versus time by considering the dynamics of governor control system. ........ 38
2.12 (a) The normalized frequencies and (b) the rotor phase angle differences versus time with flocking-based control and governor control systems. .... 39
2.13 Power transmission $P_u$ between the generators and the fast-acting ESSs in the presence of our proposed protocol and governor control systems. .... 39
2.14 (a) The normalized frequencies and (b) the rotor phase angle differences versus time with flocking-based control under the communication delay $\tau = 0.1$ s.

2.15 (a) The normalized frequencies and (b) the rotor phase angle differences versus time with flocking-based control and governor control systems under the communication delay $\tau = 0.1$ s.

2.16 (a) The normalized frequencies and (b) the rotor phase angle differences versus time with neither control nor governor control systems.

2.17 (a) The normalized frequencies and (b) the rotor phase angle differences versus time without control.

2.18 (a) The normalized frequencies and (b) the rotor phase angle differences versus time with flocking-based control.

2.19 (a) The normalized frequencies and (b) the rotor phase angle differences versus time with flocking-based control and governor control systems.

2.20 Power transmission $P_u$ between the generators and the fast-acting ESSs in the presence of our proposed protocol (a) [left] without considering governor control systems, (b) [right] considering governor control systems.

2.21 (a) The normalized frequencies and (b) the rotor phase angle differences versus time with flocking-based control under the communication delay $\tau = 0.1$ s.

2.22 (a) The normalized frequencies and (b) the rotor phase angle differences versus time with flocking-based control and governor control systems under the communication delay $\tau = 0.1$ s.

3.1 Proposed two-tier hierarchical cyber-physical integrated multi-agent framework.

3.2 Hierarchical cyber-physical control for New England 39-bus system.

3.3 (a) New England 39-bus power system, (b) Flocking-based analogy where flockmates travel through information space.

3.4 Traveling flockmates’ directed trajectory in the information space.

3.5 (a) Normalized rotor frequencies and (b) phase angles versus time of 10 s.

3.6 The trajectories of the flockmates with the observation time windows of (a) 100 ms and (b) 500 ms.

3.7 The distribution of amplitude coefficients $A_{ij}$ and initial phases $\alpha_{ij}$ for the dominant KMs with the observation time windows of (a) 100 ms and (b) 500 ms.

3.8 (a) Normalized rotor frequencies and (b) phase angles versus time of 10 s.

3.9 The trajectories of the flockmates with the observation time windows of (a) 100 ms and (b) 500 ms.
3.10 The percentage of success versus SNR value with (a) fault on Line 21 – 22 and (b) fault on Line 14 – 15.

3.11 The percentage of success versus percentage of PMUs being attacked $P_a$ with (a) fault on Line 21 – 22 and (b) fault on Line 14 – 15.

3.12 Communication between PDC and agents locally within each cluster.


3.14 (a) Normalized rotor frequencies and (b) phase angles without cyber control.

3.15 (a) Normalized rotor frequencies and (b) phase angles with the non-hierarchical control.

3.16 Power transfer $P_u$ by fast acting energy storage at generator buses in the presence of non-hierarchical control for Case Study I.

3.17 (a) The trajectories of the flockmates for Case Study I and (b) power transfer $P_u$ by fast acting energy storage at generator buses in the presence of hierarchical control for Case Study I.

3.18 (a) Normalized rotor frequencies and (b) phase angles with hierarchical control.

3.19 (a) Normalized rotor frequencies and (b) phase angles without cyber control.

3.20 The trajectories of the flockmates for Case Study II.

3.21 (a) Normalized rotor frequencies and (b) phase angles with hierarchical framework.

3.22 Power transfer $P_u$.

3.23 Performance evaluation of Cases I and II by considering physical constraints of fast-acting energy storage.

3.24 The stability margin achieved under the practical constraints in (a) Case Study I and (b) Case Study II.

3.25 Power transfer $P_u$ by fast acting energy storage at generator buses.

3.26 (a) Normalized rotor frequencies and (b) phase angles versus time.

3.27 (a) Normalized rotor frequencies and (b) phase angles with hierarchical control when considering fixed communication delay.

3.28 (a) Normalized rotor frequencies and (b) phase angles with hierarchical control when considering random communication delay.

3.29 Stability Margin $\xi$ in the situation considering (a) fixed communication delay and (b) random communication delay.

3.30 (a) The normalized frequencies and (b) the rotor phase angles versus time without proposed cyber-physical security protocol in presence of random attack.

3.31 $P_u$ versus time without proposed cyber-physical security protocol in presence of random attack.
3.32 (a) The normalized frequencies and (b) the rotor phase angles versus time with proposed cyber-physical security protocol in presence of random attack.

3.33 $P_u$ versus time with proposed cyber-physical security protocol in presence of random attack.

3.34 (a) The normalized frequencies and (b) the rotor phase angles versus time without proposed cyber-physical security protocol in presence of random attack.

3.35 $P_u$ versus time without proposed cyber-physical security protocol in presence of random attack.

3.36 (a) The normalized frequencies and (b) the rotor phase angles versus time with proposed cyber-physical security protocol in presence of smart attack.

3.37 $P_u$ versus time with proposed cyber-physical security protocol in presence of smart attack.


4.2 The wide-area multi-hop mesh network.

4.3 Flocking-based paradigm for multicast network routing in the face of DoS attack.

4.4 (a) Normalized rotor frequencies and (b) phase angles versus time without wide area monitoring and control.

4.5 GOAliE packet delivery ratio versus $(\gamma, \beta)$ for a) low congestion, b) higher congestion, c) DoS attack at Node 39 for $t \geq 5$ s, and d) DoS attack at Nodes 5 and 6 for $t \geq 5$ s.

4.6 GOAliE packet delivery ratio versus $w_1$ for a) low congestion, b) higher congestion, c) DoS attack at Node 39 for $t \geq 5$ s, and d) DoS attack at Nodes 5 and 6 for $t \geq 5$ s.

4.7 GOAliE end-to-End Latency versus packet generating time for a) higher congestion, and b) DoS attack at Node 39 for $t \geq 5$ s.

4.8 GOAliE end-to-End Latency versus packet generating time for DoS attack at Nodes 5 and 6 for $t \geq 5$ s.

4.9 (a) Normalized rotor frequencies and (b) phase angles versus time in the presence of distributed control [4] for high congestion by using GOAliE.

4.10 (a) Normalized rotor frequencies and (b) phase angles versus time in the presence of distributed control [4] for high congestion by using the unicast routing scheme [5].

4.11 (a) Normalized rotor frequencies and (b) phase angles versus time in the presence of distributed control [4] for DoS by using GOAliE.
4.12 (a) Normalized rotor frequencies and (b) phase angles versus time in the presence of distributed control [4] for DoS by using MANSI multicast routing [6].

4.13 (a) Normalized rotor frequencies and (b) phase angles versus time without wide area monitoring and control.

4.14 GOAliE packet delivery ratio versus ($\gamma$, $\beta$) for a) low congestion, b) higher congestion, c) DoS attack at Node 21 for $t \geq 5$ s, and d) DoS attack at Nodes 27 and 28 for $t \geq 5$ s.

4.15 GOAliE end-to-end latency versus packet generating time for a) higher congestion, and b) DoS attack at Node 21 for $t \geq 5$ s.

4.16 GOAliE end-to-end latency versus packet generating time for DoS attack at Nodes 27 and 28 for $t \geq 5$ s.

4.17 Normalized rotor frequencies and phase angles versus time for distributed control [4] for GOAliE: (a) and (b) in the face of high congestion and (c) and (d) DoS attack.

B.1 Modified IEEE 14-bus power system.

B.2 Normalized rotor frequencies and phase angle differences without cyber control.
List of Abbreviations

CCC  Cooperative Congestion Control
CCT  Critical Clearing Time
DER  Distributed Energy Resource
DoS  Deny-of-Service
EES  External Energy Storage
FACTS Flexible AC Transmission Systems
GOALiE Goal-Seeking Obstacle and Collision Evasion
IED  Intelligent Electronic Device
KM   Koopman Mode
LAN  Local Area Network
MWh Megawatt hours
NASPInet American Synchrophasor Initiative Network
NASPI American Synchrophasor Initiative
NERC North American Electric Reliability Corporation
PDC  Phasor Data Concentrator
PD   Positive Definite
PLC  Programmable Logic Controller
PMU  Phasor Measurement Unit
PSD  Positive Semi-Definite
QoE  Quality of Experience
QoS  Quality of Service
RTU  Remote Terminal Unit
SCADA Supervisory Control and Data Acquisition
SNR  Signal-to-Noise Ratio
STFT Short-Time Fourier Transform
WAMPAC Wide-Area Monitoring, Protection And Control
WAMS Wide Area Monitoring System
WECC Western Electricity Coordinating Council
List of Symbols

\( \alpha_i \) Binary parameter indicating lead agent
\( \omega \) Normalized relative frequency
\( \omega_l \) Normalized relative frequency of lead agent
\( \omega_s \) Normalized relative frequency of secondary agent
\( \omega_r \) Normalized relative frequency in the presence of communication delay
\( \omega_r \) Normalized reference frequency
\( \theta \) Rotor phase angle
\( \theta_l \) Rotor phase angle of lead agent
\( \theta_s \) Rotor phase angle of secondary agent
\( \theta_r \) Rotor phase angle in the presence of communication delay
\( \chi_{ij} \) Distance between flockmates
\( \delta_i \) Generator’s acceleration
\( \gamma_i \) Parameters designed in the multi-flock-based timely coherency generator identification method
\( u \) Command signal to control the fast-acting ESS
\( I_i \) Information carried by the flockmate
\( \tau \) Total communication delay for WAMS
\( \zeta_{ij} \) Feature similarity between flockmates
\( B_{ij} \) Kron-reduced equivalent susceptance
\( c_i \) Parameters designed in the flocking-based cyber-physical control protocol
\( D_i \) Generator damping parameter
\( E_i \) Internal voltage
\( g_{ii}^l \) Acceleration of Flockmate \( i \) caused by interaction with Flockmate \( j \)
\( G_{ij} \) Kron-reduced equivalent conductance
\( M_i \) Generator inertia parameter
\( N \) Number of synchronous generators
\( p_i \) Position of the flockmate
\( P_{m,i} \) Mechanical power input
\( P_{u,i} \)  Power output from the fast-acting ESS
\( S_i \)  State of the flockmate
\( T_i \)  Governor parameters
\( v_i \)  Velocity of the flockmate
\( w_i \)  Weights designed in the multi-flock-based timely coherency generator identification method
\( Y_{ij} \)  Kron-reduced equivalent admittance
Chapter 1

Introduction

1.1 Background

The National Academy of Engineering hails the electric power grid as the 20th century’s innovation most beneficial to civilization [7]. The electric power grid started in 1896, based in part on Nikola Tesla’s design published in 1888 [8]. It is the fundamental infrastructure of modern society. Transportation, communications, finance, and other critical infrastructures are dependent upon its secure, reliable electricity supplies for energy and control. The term "electric power" is the rate at which electrical energy is transferred by an electric circuit to produce useful work involving heat, light, motion, sound, information technology processes, and chemical changes. Energy is a quantity that measures the ability of a physical system to produce change on another physical system. Changes are produced when the energy is transferred from one system to another through (1) physical/thermodynamical work, (2) heat and/or (3) mass transfer. Electricity is an energy carrier. Although energy is not naturally available in the form of electricity nor is electricity directly used to produce change, its conversion to and from electricity enables the transmission of power from generation to consumption over a complex interconnected grid. The term grid in the context of power systems has traditionally been used to represent the network of electrical components used to supply, transmit and consume electric power. This term can refer to the complete or a suitable subset of electricity generation, transmission, and distribution infrastructure [9–11]. Popular grid topologies in North America are radial and mesh while loop topologies are predominant in Europe.

In recent years, electricity demand is changing and growing very fast. For example, the devices and infrastructures needed to operate the fundamental communication network, data centers, and storage alone add more than 2500 Megawatt hours (MWh) of demand globally per year that did not exist five years ago. In 2012, the average monthly electricity consumption for a U.S. residential utility customer was 903 kWhs [12]. It is expected that the world’s electricity
demand will be triple by 2050. The increasing electricity demand causes electric transmission congestion and atypical power flows threaten to overwhelm the power grids which face many challenges that they were not designed and engineered to handle. Because modern infrastructure systems are so highly interconnected, a change in conditions at any one location can have immediate impacts over a wide area, and the effect of a local disturbance even can be magnified as it propagates through a network. Large-scale cascade failures can occur almost instantaneously and with consequences in remote regions or seemingly unrelated businesses. On the North American power grid, for example, transmission lines link all electricity generation and distribution on the continent. Wide-area outages in the late 1990s and summer 2003 underscore the grids vulnerability to cascading effects [13, 14]. Furthermore, with the increasing energy demand, the modern power grid is growing into a complex network with numerous interconnected regional grids, owned and operated by power corporations at all levels and scales. The complex interests, operations, and management among different power corporations often complicate cross-region transmission tasks and sometimes result in an inefficient or poorly-coordinated power delivery. The deregulation of the energy industry necessitates high granularity of informational, financial and physical transactions to assure adequate power system operation in a competitive electricity market. However, the traditional grid has not kept pace with these modern challenges [15]. Moreover, mitigating climate change requires large-scale incorporation of renewable sources into the energy mix. The International Energy Agency predicts that hydro power will remain the major source of renewable energy for the next two decades, followed by wind and solar. The challenges of integrating these renewable energy sources into the electrical system are different for each technology but the system of the future must accommodate them all. Therefore, achieving high levels of renewables will require the systems to be more flexible, responsive and intelligent, which is substantially different from the existing grids [16]. Therefore, the existing grids are under pressure to deliver the growing demand for power, as well as provide a stable and sustainable supply of electricity. These complex challenges are driving the evolution of Smart Grids, which are considered as the next-generation electric power grids.

1.1.1 Smart Grid Visions

A smart grid, as illustrated in Fig. 1.1, can be described as the result achieved by integrating advanced control and communication technologies with the traditional power grid. Because of this integration, in a smart grid, there are both bidirectional information flow and bidirectional physical power flow. One of the key components is improved (human) operator interface and decision support. There is not yet an internationally unified definition of a smart grid. The
North American Electric Reliability Corporation (NERC) defines the smart grid as the integration and application of real-time monitoring, advanced sensing, communications, analytics, and control, enabling the dynamic flow of both energy and information to accommodate existing and new forms of supply, delivery, and use in a secure, reliable, and efficient electric power system, from generation source to end-user [17]. The marriage of information technology with traditional power grids enables the smart grids exhibit advanced functionalities. For example, by broadly deploying advanced sensors on critical components, a smart grid is able to visualize the power system in real-time. By upgrading the control and protection techniques, a smart grid is able to more effectively utilize the grids’ capacity. A smart grid is able to be situationally-aware and self-healing via wide-scale deployment of power electronic devices such as power electronic circuit breakers and Flexible AC Transmission Systems (FACTS). Furthermore, as illustrated in Fig. 1.2, the integrated communication networks in the smart grids enhance consumer-centricity such that the power delivery system is expanded by using Supervisory Control and Data Acquisition (SCADA) systems and other wide-area monitoring techniques, electricity services are improved by developing the home automation systems and enabling the real-time charging and billing information.

The smart grids’ advanced functionalities facilitate their goals on delivering high efficiency from technical, environmental, and economic perspectives. Technically, the smart grids intend to protect physical and information assets from man-made and natural threats, develop self-healing delivery infrastructure, and ensure extremely reliable delivery of “digital-grade” power to increasing numbers of end-users. From the environmental prospective, the smart grids target to reduce carbon footprint by accommodating renewable and traditional energy sources. Economically, the smart grids enhance consumer-centricity and propose affordable maintenance in order to stay globally competitive.
Besides the definition of smart grid provided by NERC, there are various alternative views of smart grids suggested by different organizations. For instance, in Electric Power Research Institute’s (EPRI’s) viewpoint, the objective of the smart grid is the convergence of greater consumer choice and rapid advances in communications, computing and electronic industries [18, 19]. The U.S. Department of Energy (DOE) denotes operating principles of the smart grid where open but secure system architecture, communication techniques and standards are used to provide value and choice to consumers [20, 21]. The smart grid criteria defined by the multinational corporation ABB includes adaptive, predictive, integrated, interactive between customers and markets, optimized to maximize reliability, availability, efficiency and economic performance, and secure from attack and naturally occurring disruptions [22]. Overall, although there is no definition of the smart grid that prevails, all the smart grid visions agree on the general theme that the smart grid aims to improve functionality of power delivery system with use of advanced technology which are both cyber and physical.

1.1.2 Security Challenges and Fundamental Questions

While the extensive integration of cyber technology with the power system significantly improves reliability and efficiency, it also introduces additional risk from cyber attacks. The security of a system is as strong as its weakest link. Thus, the high complexity of the smart grid cause the system weakness to become aggravated and result in previously unknown emergent properties. The increased connectivity provides external access to the system weakness,
which in turn can lead to compromise and infection of components. Furthermore, the tight collaboration of cyber technology and the power grid enables the attackers to increase the capabilities to exploit the system weakness. The interaction of these three components creates a host of unfamiliar vulnerabilities stemming from cyber intrusion and corruption potentially leading to devastating physical effects. For example, the first-ever control system malware called Stuxnet was found in July 2010. This malware, targeting vulnerable SCADA systems, shows that attackers have the ability to develop this type of cyber-physical attacks \[23, 24\].

From a technical perspective there is increased opportunity for cyber attack because of the greater dependence on intelligent electronic devices, communications and advanced metering amongst other intelligent systems. Such cyber infrastructure typically employs standardized information technologies that may have documented vulnerabilities. Coupled with increased economic motivations for attack that stem, in part, from privatization of the energy industry, cyber security of the smart grid represents a timely research and engineering problem.

Furthermore, enhancing the smart grid security is also important for protecting the public from terrorism, vandalistic hackers, disgruntled insiders of the electric power industry and cascading failures from the loss of other critical infrastructures. The associated attacks on availability can result in damaging instability such as blackouts and brownouts. Moreover, securing a smart grid makes business sense. Protection of cyber devices is necessary to establish compliance to cyber security requirements to be able to compete in the electricity marketplace. Security also represents a means to reduce or divert technical liability and assure revenue by discouraging competitor component cloning.

Numerous reports are appearing which acknowledge current security concerns of the smart grid \[25–30\]. Some guidelines have also been published by government agencies and other authoritative organizations, such as NISTIR 7628 Guidelines for Smart Grid Cyber Security developed by the National Institute of Standards and Technology (NIST) \[31\], the document Roadmap to Achieve Energy Delivery System Cyber Security released by the DOE \[32\], and Critical Infrastructure Protection (CIP) standards proposed by the NERC \[33\]. These reports and guidelines raise three fundamental research and development questions for improving the smart grid security: (1) What are the electrical system impacts of a cyber attack? (2) How should security resources be prioritized for the greatest advantage? (3) Is the additional information available through advanced cyber infrastructure worth the increased security risk? Moreover, two main concerns on cyber attacks are specified by the reports and guidelines: (1) the possibility of attacks on information accuracy such as the false data injection attacks, and (2) the possibility of attacks on timely data delivery such as denial of information access on the SCADA control system.
1.2 Literature Review

Recently, smart grid researchers have been trying to develop potential solutions for the fundamental questions to enhance the smart grid security. It has been realized that security vulnerability analysis for the smart grid is able to aid in answering those questions. Cyber attacks on the smart grid, commonly classified as either outsider or insider, can occur within devices or along the communications paths of the cyber infrastructure. To address outsider attacks, in which an opponent has no specialized security information such as secret keys, mechanisms for authentication, access control, data integrity, confidentiality and non-repudiation suitable for smart grid infrastructure are being developed [34–71]. Essentially, cryptographic primitives are applied to make such attacks either practically impossible or detectable thus alerting appropriate parties of an attack. The problem of insider attacks, in contrast, involves a trusted but corrupted entity such as a smart meter that has full access to secret keying information; here, the corrupted entity can apply numerous attacks such as falsification or delaying of data and go undetected possibly for some time or until, for example, a power delivery disruption occurs. Typically, it is difficult to immediately identify the exact source of a cyber attack and mechanisms such as islanding can be applied to isolate the corrupted components from causing large-scale disruption [72].

Research focused on cyber security often takes an information-centric perspective in which data protection is of paramount importance [73]. For smart grid applications where consumer-centricity is emphasized, efficient and safe power delivery services are a more significant concern to stakeholders than the health of the support-data used to control it. It is possible that investment in cyber security that leads to improvements in information technology has only negligible advantage for the power system [52]. It is therefore important to focus on assessing the impacts of cyber attacks on the electricity network to identify possible new vulnerabilities, develop countermeasures and prioritize mitigation investment. Initial research into cyber security of power systems focused solely on the cyber infrastructure [34–71]. It is true that protection of the data better facilitates a safer electrical grid. However, because of the limited resources of electric power utilities, it is also necessary to understand the cost-benefit trade-offs of protection mechanisms. Proper smart grid risk analysis necessitates that vulnerability assessment take into account the physical impacts of cyber attack [74, 75]. Thus recently there has been a movement to incorporate cyber-physical information. For emerging smart grid topologies this interface commonly occurs at the sensors and actuators, such as intelligent electronic devices (IEDs), remote terminal units (RTUs), programmable logic controllers (PLCs), that are acquiring data from and using data to control electrical components [76–81].

Recently, power system cyber security research thrusts have focused on modeling this
unique cyber-to-physical bridge for a smart grid which aids in analyzing the impact of cyber attack on the power system. These techniques can be grouped into a number of classes. One class of static methodologies identify the cause-and-effect relationships within the cyber-to-physical bridge [82–84] to relate one or more cyber attacks to one or more physical consequences that are further analyzed using power system-specific tools. To account for the effects of time scale and timing on the overall system security, one class of empirical approaches has focused on merging well-developed simulators/emulators for the communications infrastructure, power systems, and control centers [48, 85, 86, 86–89] to account for the dynamic nature of the interactions. These two forms of simulators are combined such that an attack is applied in the communication simulator that transfers data to the power systems simulator which makes decisions based on this possibly corrupt information. Typical traditional power system reliability metrics are used to assess impact of the cyber attacks. In cyber-physical leakage approaches confidentiality of the cyber network is studied by identifying how voltage and current measurements of the physical power system can be analysed for any clues about cyber protocol activity [90–93, 93, 94]. Similarly, such contextual information relating cyber and physical dependencies have been exploited for intrusion detection [95–98, 98, 99]. Testbed systems research addresses the exploration of practical vulnerabilities through SCADA testbed development and construction [100–102]. Much of this valuable research has proven that cyber attacks have the potential to cause significant disruptions in power delivery. However, the individual cyber and electrical simulators are often incompatible for study within a common framework. Commonly, exhaustive searches must be employed in order to understand worst-case scenarios. Attempts to provide more analytic insights into the problem for general feedback control system architectures have also been pursued [103, 104, 104–106], which focuses on how data corruption of denial of information access can affect the control of the power grid. Finally, the research in [107, 108] represented a work in progress towards the development of a comprehensive and practical framework for electric smart grid cyber attack impact analysis.

1.3 Problem Statement and Thesis Objectives

In order to secure emerging systems such as the smart grid, it is important to identify and characterize the existing and new forms of vulnerabilities before making critical design decisions. Moreover, important questions arise when identifying priorities for protection: (1) What are the electrical system impacts of a cyber attack? (2) How should security resources be prioritized for the greatest advantage? (3) Is the additional information available through advanced cyber infrastructure worth the increased security risk? Due to the highly complex cyber-physical nature of the smart grid, the simple combination of pure information (cyber) processing and pure
energy (physical) processing is inefficient for characterizing the smart grid vulnerabilities and answering the fundamental research and development questions. We assert that to unify the discrete and analog aspects of the smart grid one must account for their salient cyber-physical coupling. Some research has been developed on modeling the unique cyber-physical bridge for a smart grid to aid in vulnerability assessment and protection design. However, the existing work still demonstrates a large degree of decoupling. Cyber and physical information are described in different languages and the modeling techniques are not holistic.

Our research aims to enable the tighter coupling between the cyber and physical entities while addressing security issues of the smart grids. In order to achieve this goal, the research work presented in this thesis seeks to develop a biologically-inspired dynamic systems paradigm with the following objectives:

1. To develop a biologically inspired dynamic model to describe smart grid cyber-physical interactions in a common language, which enables the convenient description of (discrete) cyber and (analog) physical couplings.

2. To propose a secure cyber-physical control strategy using distributed generators and storage to re-stabilize a smart grid system under various forms of cyber and physical attack.

3. To propose a witness-based security protocol for identifying and mitigating the information corruption.

4. To design a biologically inspired multicast routing approach for synchronous data delivery in Smart Grids, which is resilient to Denial-of-Service (DoS) attack and network congestion.

1.4 Methodology

As illustrated in Fig. 1.3, in order to achieve our research objectives, we make use of the toolsets consisting of graph theory, dynamical-system formulation, and flocking rules. A graph is defined by a collection of vertices (also called nodes) and a collection of edges that connect node pairs. It is a mathematical structure that represents pairwise relationships between a set of objects. Depending the use of a graph, its edges may or may not have direction leading to directed or undirected classes of graphs, respectively. Graphs provide a convenient and compact way to describe the cyber-physical interactions and relate dependencies within a power system as witnessed by recent papers that use this tool [88, 109, 110]. However, as stated in [109], purely graph-based approaches do not sufficiently model the state changes within the physical system. Moreover, they do not effectively account for the unique characteristics of the system.
at various time-scales nor provide a convenient framework for modeling system physics. We assert that modeling the electrical grid is a vital component to an effective impact analysis framework.

One approach to physically modeling complex engineering interactions employs dynamical systems. A dynamical system is a mathematical formalization used to describe time-evolution of a system state, which can typically represent a vector of physical quantities. As shown in Fig. 1.3, \( x \) denotes the physical state of the system. Because of the physical characteristics of power system, the time-evolution of \( x \) is described by the following differential equation:

\[
\dot{x} = f(x, u),
\]

where \( \dot{x} \) is the time-derivative of \( x \), \( u \) is the control input obtained by the cyber-physical interaction, and the function \( f(\cdot) \) is determined by the power system network topology in our work.

Dynamical systems theory is motivated, in part, by ordinary differential equations and is well-suited to representing the complex physical interactions of the power grid. Furthermore, \( s \) in Fig. 1.3 represents the cyber measurement of the system and the measurement function \( g(\cdot) \)
in our work is formulated as follows:

\[ g(s) = s + n, \]

where \( n \) denotes the random environment noise. Therefore, the graphs and dynamical systems tool-sets enable a cyber-physical dynamic graph representing the cyber and physical grid entity relationships in a smart grid. As shown in Fig. 1.3, in the graph, the state change of each cyber-physical node can be formulated by a dynamic function \( f(\cdot) \) of the physical state \( x \) and the cyber-physical control input \( u \). We clarify that although our research does not target at achieving complete state controllability and observability, the efficiently designed cyber-physical integration in our work, such as the wisely located PMUs obtaining the measurement \( s \) and the proposed cyber-physical control protocol achieving \( u \), achieves sufficient controllability and observability for the application of maintaining smart grid stability.

However, the design of the control protocol \( h(\cdot) \) is a big challenge due to the complex networked characteristics and resilience requirements of smart grids. Fortunately, flocking behavior in the nature sheds light on the robust distributed control design for complex systems. The collective behavior coordination and local interaction in flocks contribute to an effective solution for accomplishing the system objectives via robust distributed control and communication. Furthermore, the emergent behavior in flocks, such as obstacle avoidance, provides an essential idea to achieve the situational-awareness in real-time for smart grids.

We assert that the tool sets consisting of graph theory, dynamical-system formulation, and flocking behavior are effective for a smart grid vulnerability assessment and security design for a variety of reasons. First, effective smart grid attack analysis necessitates relating the cyber attack to physical consequences in the electricity network. A dynamical systems paradigm provides a flexible framework to model (with varying granularity and severity) the cause-effect relationships between the cyber data and the electrical grid state signals and ultimately relate them to power delivery metrics. Second, graphs enable a tighter coupling between the cyber and physical domains. For a smart grid, the cyber-to-physical connection is often represented through control signals that actuate change in the power system and the physical-to-cyber connection is typically due to the acquisition of power state sensor readings. These connections can be conveniently expressed as specifically located edges of the graphs. This way cascading failures and emergent properties from the highly coupled system can be represented. Mitigation approaches such as active control or islanding of the grid or partitioning of the core smart grid components for optimal functions, and a graph-based dynamical systems formulation can naturally portray such separation as well. Third, the flocking behavior exhibits novel and essential principles to efficiently design the security strategies for an overall system resilient to
cyber and physical disruption. Last, a primary effect of including cyber attacks in traditional reliability analysis is that it increases the size of the system under study by several orders of magnitude. Our proposed mathematical formulation has the potential to keep studies tractable because our granularity of detail can be tuned and the use of dynamics can enable sophisticated behaviours without a corresponding increase in complexity.

1.5 Dissertation Outline

This dissertation consists of six chapters and one appendix. Figure 1.4 show the outline of the dissertation. We first present the flocking-based cyber-physical dynamical systems paradigm for smart grid analysis as shown in Chapter 2. In order to reduce the information acquisition in smart grids, we extend the work in Chapter 2 and achieve a two-tier hierarchical cyber-physical security analysis framework, which is presented in Chapter 3. In order to address attacks on information accuracy and on timely data delivery, we propose a witeness-based security protocol and a resilient multicast routing approach: Goal-Seeking Obstacle and Collision Evasion (GOALiE) in Chapters 3 and 4.

Figure 1.4: Dissertation Outline.

Chapter 2 proposes a flocking-based cyber-physical dynamical systems paradigm to model
the cyber-physical interactions related to smart grid stability. In our multi-agent framework each node, representing both electrical and information system components, is modeled as having dynamics that synergistically describe physical and information couplings with neighboring agents. Physical behaviors are described through the application of swing equations to a reduced model of the electrical grid. Cyber-physical integrated action is formulated as a flocking control problem to achieve smart grid stability. The cyber-physical flavor of our framework enables the simultaneous study of both physical disruptions as well cyber impediments. We study both analytically and empirically the impact of information delay on our flocking-based control strategy and illustrate how the inherent robustness of flocking behavior provides a natural fortitude against communication bottlenecks and interruption. Analysis and simulation demonstrate the potential of the paradigm to model cyber-physical smart grid dynamics as well as highlight strategies for effective distributed control.

Chapter 3 demonstrates one approach to harness physical couplings within a power grid system to enable the selective use of cyber data acquisition and distributed control using a flocking-based paradigm. Within the two-tier multi-agent framework, distributed cyber-control is applied at lead generators to achieve first-tier smart grid stability. Physical coherence is exploited with a novel multi-flock-based coherency identification technique so that secondary agents coupled to lead agents also achieve second-tier synchronization. Analysis and empirical results support our approach. Furthermore, this chapter also presents a witness-based security protocol that considers a cyber-physical perspective to the problem of identifying and mitigating information corruption in smart grid systems. We study the problem of smart grid stability with distributed control using real-time data from geographically distributed PMUs via a flocking-based modeling paradigm. We demonstrate how cyber corruption can be identified through the effective use of telltale physical couplings within the power system. We develop a novel witness-based cyber-physical protocol whereby physical coherence is leveraged to probe and identify PMU data corruption and estimate the true information values for attack mitigation.

Chapter 4 develops GOAliE an approach to resilient multicast routing for smart grid applications based on principles from robust flocking theory. We assert that analogies exist between the flocking principles of goal seeking, obstacle evasion, collision avoidance and behavioral transitions and the routing goals of low latency, buffer overflow management and adaptability in the presence of changing network conditions. Our multicast routing framework employs an underlying dynamical systems model convenient for integration with representations of power system dynamics to produce an overall cyber-
physical smart grid description. Through simulations and comparisons with prior art we demonstrate how our approach provides insight on effective multicast routing principles to promote resilience in faulted power systems in the presence of congestion and denial-of-service attacks on communications infrastructure.

Chapter 5 summarizes the conclusions of this dissertation, discusses its contributions, and recommends the future research directions.

Appendix A overviews the fundamental concepts in graph theory.

Appendix B presents an alternative generator coherency identification technique, Special Matrix-based Agent Coherency Identification Approach.
Chapter 2

Flocking-Based Cyber-Physical Dynamical Systems Paradigm

2.1 Introduction

Electric power utilities currently reside in an environment of increasing power demand, market deregulation and a growing movement towards sustainability. Consequently, utilities have been driven to reduce operating margins pushing power systems to exhibit greater nonlinearity. Moreover the movement towards a smarter grid integrates sophisticated information systems within this already complex network. We assert that fundamental models that strengthen the scientific basis of smart power systems are needed to better understand the associated cyber-physical interactions.

Recent work has proposed finding a balance between dynamical representations and models found in network science [107, 111–114]. In this spirit, we build upon well known dynamical models of power systems recently employed in [113] and incorporate cyber intelligence and control behaviors by taking a flocking perspective commonly used to model large-scale natural phenomenon.

We assert that our multi-agent flocking-based approach has the following advantages. First it enables the convenient integration of cyber (communications and control) systems within dynamical models of power system physics. Second, the structure of our models conveniently enables the study of the important smart grid stability problem. Third, the models of cyber system dynamics can be employed to gain insight on effective smart grid distributed communications and control strategies for system performance and stabilization.

Our research carries the flavor of recent work by Dörfler and Bullo [113] and Feng et al. [115] by applying cooperative control strategies to power systems with the following dis-
tinctions. We incorporate cyber system dynamics into our formation thus enabling character-
izations of cyber-physical dependencies of importance to smart grids. The flocking paradigm
allows communications and control goals to be elegantly abstracted within models of the phys-
ical power system to aid in the study of system operation and control. Moreover we are able
to relax the overdamped generator assumption of [113] through the effective design of cyber
dynamics.

Furthermore, we study the robustness of our approach from two perspectives. First, we
study how our flocking-based control approach increases the critical clearing time in contrast
to purely passive approaches of clearing the fault. Then, we analyze the ability of the control
to enable smart grid stability even in the presence of communication delay. This is especially
important in emerging wide area monitoring systems (WAMS) in which communication delays
may be present due to natural system latency and even intentional denial-of-service (DoS)
attack.

### 2.2 Dynamic Multi-Agent System Framework for Cyber-Physical
Integration Modeling

#### 2.2.1 Smart Grid Stability

In our research, we consider the smart grid stability from the power system (physical) perspec-
tive, which can be seriously impacted by the cyber-physical interactions in the system. The
power system stability is defined as the ability of an electric power system, for a given initial
operating condition, to regain a state of operating equilibrium after being subjected to a dis-
turbance, with all system variables bounded so that system integrity is preserved [3, 116]. As
shown in Fig. 2.1, there are three types of stability are considered for power systems: rotor
angle stability, frequency stability, and voltage stability. Furthermore, rotor angle stability and
frequency stability are associated with active power control, and voltage stability is associated
with reactive power control. Our research focuses on active power control and targets at im-
proving the rotor angle stability and frequency stability of the system in the face of large system
disturbance.

#### 2.2.1.1 Rotor Angle Stability

Rotar angle stability describes the ability of the interconnected synchronous generators to re-
main in synchronism under normal conditions and after being subjected to a disturbance. The
rotor angle stability of a power system depends on the ability to maintain the equilibrium
between electromagnetic torque and mechanical torque of each synchronous machine in the system. Under a steady state condition, each generator remains in a constant speed and its input of electromagnetic torque and mechanical torque is balanced. If the system is perturbed, the equilibrium is upset, resulting in acceleration or deceleration of the rotors of some generators leading to their loss of synchronism with other generators. Beyond a certain threshold $\gamma$, an increase in angular separation is followed by a decrease in power transfer such that the angular separation is increased further, which leads to instability. Rotor angle stability can be characterized in terms of the following two subcategories:

1. Small-signal rotor angle stability refers to the ability of the power system to maintain synchronism under small disturbances. The disturbances are considered to be sufficiently small such that linearization of system equations is commonly implemented for the purpose of analysis. The time frame of interest is usually 10 to 20 seconds following a disturbance.

2. Transient stability refers to the ability of the power system to maintain synchronism when subjected to a severe disturbance. The resulting system response involves large excursions of generator rotor angles and thus the nonlinear power-angle relationship has to be considered for the purpose of analysis. The time frame of interest is usually 3 to 5 seconds following the disturbance.

2.2.1.2 Frequency Stability

Frequency stability describes the ability of a power system to maintain steady frequency $f_0 = 60$ Hz within a permissible range following a severe system disturbance. The frequency stability of a power system depends on the ability of restoring the equilibrium between
system generation and load. Frequency stability problems are usually caused by inadequacy of the system utilities to respond to disturbances, lack of control coordination and advanced protection devices. The time frame of interest ranges from one second to minutes depending on the control and device response.

2.2.1.3 Definition of Smart Grid Stability

Let $\theta_i(t)$ denote the rotor phase angle of Generator $i$ at time $t$ and $\omega_i$ be the normalized relative frequency of Generator $i$ with respective to $f_0$ at time $t$. Based on the definitions and requirements of rotor angle stability and frequency stability, we are able to characterize the smart grid stability which is of interest to our research as follows:

**Smart Grid Stability:** a smart grid is able to achieve both phase angle cohesiveness and exponential frequency synchronization within 1 to 3 seconds following a severe disturbance:

1. Phase angle cohesiveness:

   $$|\theta_i(t) - \theta_j(t)| \leq \gamma, \text{ for } \forall t,\ (2.1)$$

   where the threshold $\gamma$ is normally set as $5\pi/9$ in the realistic application as discussed in [117];

2. Exponential frequency synchronization:

   $$\omega_i(t) \to 0, \text{ as } t \to \infty. \ (2.2)$$

2.2.2 Graph-Theoretic Dynamical Modeling for Cyber-Physical Integration

2.2.2.1 Power System Topology Reduction Analysis

Because of the fact that the synchronous generators and the dynamic loads are the critical physical components for maintaining smart grid stability, we aim to abstract the information on the physical coupling between these critical components. We employ the kron-reduction technique to characterize the power system with a graph $G$ whose vertices represent the critical physical components and the edges depict the physical coupling between the critical components. Fundamental concepts in graph theory are introduced in Appendix A.

We can always describe a power grid topology directly by a graph whose vertices represent the buses of the power system and edges represent the transmission lines. Consider a connected power grid with $N$ nodes and branch admittances $Y_{ij}$. By using Kirchhoff’s and Ohm’s
laws [118, 119] the current-balance equations are obtained as follows:

\[ \mathbf{I} = \mathbf{YV}, \tag{2.3} \]

where \( \mathbf{I} \in \mathbb{R}^{N \times 1} \) are the currents injected at the nodes, and \( \mathbf{V} \in \mathbb{R}^{N \times 1} \) are the nodal voltages.

The admittance matrix \( \mathbf{Y} \in \mathbb{R}^{N \times N} \) also represents the Laplacian matrix associated with the graph \( \mathcal{G} \). Let \( \alpha \subseteq \mathcal{V} \) be the set of vertices corresponding to the critical physical components and \( \beta = \{i \in \mathcal{V} : i \notin \alpha \} \). Equation (2.3) can be partitioned as follows:

\[
\begin{bmatrix} \mathbf{I}_\alpha \\ \mathbf{I}_\beta \end{bmatrix} = \begin{bmatrix} \mathbf{Y}_{\alpha\alpha} & \mathbf{Y}_{\alpha\beta} \\ \mathbf{Y}_{\beta\alpha} & \mathbf{Y}_{\beta\beta} \end{bmatrix} \begin{bmatrix} \mathbf{V}_\alpha \\ \mathbf{V}_\beta \end{bmatrix}. \tag{2.4} \]

Since there is no current injection at the buses corresponding to the vertices in \( \beta \), we are able to apply the kron-reduction technique to eliminate the vertices in \( \beta \) and achieve the current-balance equation associated with the reduced graph as follows:

\[ \mathbf{I}_\alpha = \mathbf{Y}_{\text{red}} \mathbf{V}_\alpha. \tag{2.5} \]

where the reduced admittance matrix \( \mathbf{Y}_{\text{red}} \in \mathbb{R}^{|\alpha| \times |\alpha|} \) can be calculated as follows:

\[ \mathbf{Y}_{\text{red}} = \mathbf{Y}_{\alpha\alpha} - \mathbf{Y}_{\alpha\beta} \mathbf{Y}_{\beta\beta}^{-1} \mathbf{Y}_{\beta\alpha}. \tag{2.6} \]

Figure 2.2 illustrates an example of the power system topology reduction analysis for the Western Electricity Coordinating Council (WECC) 3-Generator System. The critical physical components of WECC 3-Generator System are the three generators. By employing the kron-reduction technique, we achieve a reduced graph with three vertices representing the three generators and three edges describing the physical couplings between the generators. The reduced graph provides a convenient and compact way to characterize the physical interaction between the critical components in this power system.

The Laplacian matrix of the reduced graph can be calculated as follows:

\[
\mathbf{Y}_{\text{red}} = \begin{pmatrix} Y_{11} & Y_{12} & Y_{13} \\ Y_{21} & Y_{22} & Y_{23} \\ Y_{31} & Y_{32} & Y_{33} \end{pmatrix} = \begin{pmatrix} 0.4554 - 3.8232i & 0.3037 + 1.6497i & 0.4276 + 1.1942i \\ 0.3037 + 1.6497i & 0.2229 - 3.2933i & 0.3194 + 0.9750i \\ 0.4276 + 1.1942i & 0.3194 + 0.9750i & 0.4592 - 3.1195i \end{pmatrix}. \]

### 2.2.2.2 Dynamical Description

The time evolution of the states of the power system can be described by the dynamical behaviours of the critical components in the system and represented by the dynamics of the ver-
2.2.2.3 Cyber-Physical Integration Framework and Dynamical Description

Based on the achieved dynamic graph providing an abstract representation of the power system, we are able to design a cyber-physical integrated framework in which the cyber and physical systems work synergistically such that the bidirectional cyber information and power flows are efficiently used to enhance system resilience. As stated in [14], the essential characteristics of a smart grid include: 1) situational awareness in real time, 2) energy storage used and controlled to support system goals, 3) distributed control and protection integrated with other functional units. According to these characteristics, we design our networked multi-agent-based framework that integrate both cyber and physical elements as illustrated in Fig. 2.3.
Figure 2.3: Proposed multi-agent dynamic system model.
Our model is comprised of cyber-physical agents, each consisting of: (1) a dynamic node representing the critical physical component in the power system, in our work a synchronous generator, (2) a phasor measurement unit (PMU) used to deliver the characteristic of situational-awareness by acquiring generator rotor phase angle and frequency data from the dynamic node, (3) a phasor data concentrator (PDC) implemented to guarantee synchronization of the data information flows in the system, and (4) a local cyber-controller used to achieve the characteristic of distributed control and protection by computing a control signal that is applied to the generator node with PMU data. The frequency and rotor phase angle of each agent are those of its generator. The PMU and local controller are both considered to be cyber elements due to their data acquisition, communication and computation tasks. Since our focus is on the smart grid stability problem, the objective of the local controller is to achieve generator phase angle cohesiveness and exponential frequency synchronization in the face of cyber-physical disturbance. As such, the local controllers may require fast-acting External Energy Storages (EESs) in order to achieve their objectives as shown in Fig. 2.3. These storages in practice may include battery storage devices, flywheels, renewable energy sources, and other types of massive energy storage [120, 121], and may be separate from each agent. Figure 2.4 shows a example of our proposed cyber-physical multi-agent dynamic system framework by using WECC 3-Generator Power System. The red dashed arrows represent local communications within each agent, the blue dashed and solid arrows represent the communication and power transfer with the fast-acting EES, respectively, and the magenta dashed arrows represent the synchronous data information flows in the system.

The cyber network consisting of PMU information and local controllers is integrated into this framework through the injection of a control input to the right side of Eq. (2.7) to give:

\[
M_i \dot{\omega}_i = -D_i \omega_i + P_{m,i} - E_i^2 G_{ii} - \sum_{j=1}^{N} P_{ij} \sin (\theta_i - \theta_j + \varphi_{ij}) + \overbrace{u_i}^{\text{control input}}
\]  

(2.8)

where the control signal \( u_i \) is computed as a function of the data acquired by all the PMUs in the system and is used to control the power output \( P_{u,i} \) of the associated fast-acting ESS, \( \theta_j, \omega_j \) for \( j \in \{1, 2, ..., N\} \). Since normally the communication delay between the local controller and the associated fast-acting ESS is negligible, we have that \( u_i = P_{u,i} \).

Thus, the dynamics of Eq. (2.8) represents both cyber and physical interactions. Here the physical-to-cyber bridge exists at the measurement devices in which physical phase angle and frequency are converted to PMU data and the cyber-to-physical bridge occurs when the cyber-computed control signal \( u_i \) is applied to control the associated fast-acting ESS to absorb \( (u_i < 0) \) or inject \( (u_i > 0) \) the physical power \( P_{u,i} \) into the generator network. The model of
Figure 2.4: Proposed cyber-physical multi-agent dynamic system framework for the WECC 3-Generator Power System.
u_i as a function of PMU data represents the contribution of the cyber network to the overall framework. For normal system operation u_i = 0. However, when a disturbance strikes, u_i will excite the system to re-achieve (transient) stability. Computation of u_i is dependent on the overall controller goals that we discuss in the next section.

### 2.3 Flocking-Based Cyber-Physical Control Protocol Design

#### 2.3.1 Flocking Theory and Formation Control

In a system comprised of a large number of coupled agents, flocking refers to an aggregate behavior amongst the entities to achieve a shared group objective. In [122], Reynolds introduced three heuristic rules that led to the creation of the first computer animation of flocking:

1. **Flock Centering**: agents attempt to stay close to nearby flockmates,
2. **Velocity Matching**: agents attempt to match velocity with nearby flockmates,
3. **Goal Seeking**: each agent has a desired velocity towards a specified position in global space.

Based on these three rules, Olfati-Saber [123] provided a framework for design and analysis of scalable distributed flocking algorithms using a double integrator model:

\[
\begin{align*}
\dot{q} &= p \\
\dot{p} &= u,
\end{align*}
\]  

(2.9)

where \( q \in \mathbb{R}^N \) is the position vector of the flockmates, \( p \in \mathbb{R}^N \) denotes the velocity vector, \( u \in \mathbb{R}^N \) represents the control signal, and \( N \) is the size of the flock.

To achieve the objectives of flocking, the control signal \( u \) is comprised of three terms:

\[
u = -\nabla V(q) - L \cdot p + F(p, q, p_r, q_r).
\]  

(2.10)

The first term is the gradient of a potential energy function \( V(q) \) which characterizes system objectives and constraints. The second term represents a velocity consensus protocol where \( L \) is the Laplacian matrix associated with the flock communication graph. Finally, the third term models navigational feedback which is designed to ensure each agent tracks a reference \((p_r, q_r)\).

The stability of the control protocol described in Eq. (2.10) has been analyzed in [123] to provide the following sufficient conditions for stability: (1) \( V(q) \) is a nonnegative continuously
differentiable potential energy function that achieves the global minimum at a desired formation; (2) \( L \) is a standard Laplacian matrix, which is positive semidefinite and has a zero row sum \([124]\); (3) \( F(p, q, p_r, q_r) \) is a linear combination of \((p - p_r)\) and \((q - q_r)\).

### 2.3.2 Cyber-Physical Control Protocol Design by Analogy to Flocking

By studying the three flocking rules, we notice that *flock centering* is analogous to the *phase angle cohesiveness* objective in the smart grid stability problem, and the combined result of *velocity matching* and *goal seeking* is analogous to the *exponential frequency synchronization* objective in the smart grid stability problem. This analogy inspires us to reformulate the problem of smart grid stability as a task of flocking formation control. From Eq. (2.8) we delineate the cyber coupling (cyber §) and physical coupling (phys §) amongst agents as:

\[
M_i \ddot{\theta}_i = -D_i \dot{\theta}_i + P_{m,i} - E_i^2 G_{ii} - \sum_{j=1}^{N} P_{ij} \sin \left( \theta_i - \theta_j + \varphi_{ij} \right) \left( \omega_i - \omega_j \right) + u_i. 
\]

Thus, the problem of representing the collective cyber-physical dynamics of the agents requires the effective design of \( u_i \) to model the influence of the cyber network via distributed controllers common in emerging smart grid systems.

For development of the cyber control dynamics \( u_i \), we make two assumptions. First, we assume that the rate of change of \( u_i = P_{u,i} \) is much larger than that of the mechanical power input \( P_{m,i} \) for each agent and the time span to recover transient stability is short; thus we treat \( P_{m,i} \) as a constant. This assumption is reasonable for future smart grid systems where fast-response ESSs such as battery storage devices and flywheels will be available to inject and absorb energy for periods of brief control. Second, we assume that the problems of voltage regulation and transient stability are decoupled. This enables us to consider the voltage \( E_i \) as a constant during controller excitation to re-achieve the transient stability.

Under these assumptions, computing the derivatives of the both sides of the equation above (or Eq. (2.8)), the system dynamics may be reformulated as:

\[
\begin{align*}
\dot{\theta}_i &= \omega_i, \\
D_i \dot{\omega}_i &= -M_i \dot{\omega}_i - \sum_{j=1}^{N} P_{ij} \cos \left( \theta_i - \theta_j + \varphi_{ij} \right) \left( \omega_i - \omega_j \right) + u_i.
\end{align*}
\]

The system of Eq. (2.11) is not feedback linearizable due to the presence of the \( M_i \ddot{\omega}_i \) term \([125]\). Moreover, it is not appropriate to apply singular perturbation analysis since in typical practice \( M_i \in [2s, 12s]/(2 \pi f_0) \) and \( D_i \in [1s, 3s]/(2 \pi f_0) \); thus, the perturbation parameter \( \epsilon =
\( \frac{M_{\text{max}}}{D_{\text{min}}} \in \mathcal{O}(10) \) [125]. In order to overcome this obstacle, we design \( u_i \) as follows:

\[
    u_i = -D_i \sum_{j \in \mathcal{N}_i} b_{ij} (\omega_i - \omega_j) - \sum_{j \in \mathcal{N}_i} g_{ij} (\theta_i - \theta_j) + h (\theta, \omega)
\]  

(2.12)

where \( b_{ij} \) is a parameter used to facilitate singular perturbation as we discuss later, \( g_{ij} > 0 \) is a control parameter, \( \mathcal{N}_i \) denotes the index set of the neighbors of the \( i \)th agent, and \( h(\cdot) : \mathbb{R}^N \times \mathbb{R}^N \to \mathbb{R} \) is a function of the vector \( \theta = \{\theta_1, \ldots, \theta_N\} \) and the vector \( \omega = \{\omega_1, \ldots, \omega_N\} \).

Based on Eq. (2.12), we can rewrite the second line of Eq. (2.11) as follows:

\[
    D_i \left( 1 + \sum_{j \in \mathcal{N}_i} b_{ij} \right) \dot{w}_i - D_i \sum_{j \in \mathcal{N}_i} (b_{ij} \dot{w}_j) = -M_i \ddot{w}_i - \sum_{j=1}^N [P_{ij} \cos (\theta_i - \theta_j + \varphi_{ij})
\]

\[
    + g_{ij} (\theta_i - \theta_j)] (\omega_i - \omega_j) + \frac{d}{dt} h (\theta, \omega)
\]

where we assign the parameters \( \{b_{ij}\} \) to satisfy \( \epsilon = \frac{M_{\text{max}}}{\left[ D_{\text{min}} \left( 1 + \sum_{j \in \mathcal{N}_i} b_{ij} \right) \right]} \in \mathcal{O}(0.1) \).

This enables us to utilize singular perturbation techniques to study the dynamics of our networked multi-agent system of Eq. (3.3) over a longer time scale. We can rewrite Eq. (3.3) in the vector form as follows:

\[
\left\{ \begin{array}{l}
    \dot{\theta} = \omega, \\
    \dot{\omega} = -\mathcal{M}^{-1} (L + G) \omega + \mathcal{M}^{-1} \nu.
\end{array} \right.
\]  

(2.13)

where \( \mathcal{M} = D \Psi, \Psi = (I + B) \), \( I \) is an identity matrix, \( D = \text{diag} [D_1, \ldots, D_N] \), \( B = [b_{ij}] \) and \( G = [g_{ij}] \) are our proposed \( N \times N \) cyber control matrices, \( L \) is a \( N \times N \) physical coupling matrix whose elements can be represented as:

\[
    l_{ij} = \begin{cases} 
    \sum_{j \neq i} P_{ij} \cos (\theta_i - \theta_j + \varphi_{ij}), & \text{if } i = j; \\
    -P_{ij} \cos (\theta_i - \theta_j + \varphi_{ij}), & \text{if } i \neq j,
    \end{cases}
\]  

(2.14)

and \( \nu \) is a \( N \)-dimensional column vector such that the \( i \)th element is given by \( \nu_i = \frac{d}{dt} h (\theta_i, \omega_i) \).

It is straightforward to show that the matrices \( L, G \) and \( B \) all have the trivial eigenvalue 0 with corresponding eigenvector \( I \), and the matrix \( \Psi \) is a row stochastic nonnegative matrix which has a trivial eigenvalue 1 and the corresponding eigenvector \( I \) [124].

Since the nonlinear dynamical system of Eq. (2.13) is feedback linearizable, we can define
a new control vector $\tilde{u}$ and rewrite the equivalent reduced order model as:

$$\begin{align*}
\dot{\theta} &= \omega, \\
\dot{\omega} &= e u.
\end{align*}$$

(2.15)

Furthermore, we can represent the relationship between the original control vector $u$ and the new control vector $\tilde{u}$ as:

$$\dot{u} = \tilde{D} (\tilde{u} + L \omega),$$

where $\tilde{D}$ is a $N \times N$ diagonal matrix with $d_{ii} = 1/D_i$.

### 2.3.3 Design by Analogy to Flocking

Eq. (2.15) represents a double integrator system analogous to Eq. (2.9) known to model the standard dynamics of flockings. By setting $\tilde{u}$ to the following form we thus ensure flocking formation and hence transient stability of the power network:

$$\tilde{u} = -M^{-1} \nabla V(\theta) - \tilde{L} \omega + M^{-1} F(\omega, \omega_r),$$

(2.16)

where $V(\theta)$ represents the potential energy function to guarantee that the phase angle differences between pairs of agents are bounded, $\nabla V(\theta)$ is its associated gradient with respect to $\theta$, $\tilde{L}$ is the effective Laplacian matrix that ensures frequency consensus (i.e., agents’ frequencies converge to a common value), and $F(\cdot)$ is the navigation feedback designed to “lead” the frequencies to converge to the desired value $\omega_r$; typically relative frequency is normalized such that $\omega_r = 0$.

#### 2.3.3.1 Potential Energy Function

Based on the sufficient condition of Eq. (2.1), we consider the following potential energy for our control scheme:

$$V(\theta) = \frac{1}{2} \sum_i \sum_{j \neq i} \psi(\theta_i - \theta_j),$$

(2.17)
where \( \psi(\cdot) \) is a pairwise attractive potential defined as based on the requirement of phase angle cohesiveness stated in Section 2.2.1.3:

\[
\psi(z) = \begin{cases} 
0, & \text{if } |z| \leq \frac{5\pi}{9}; \\
c_1 \left( z^2 - \frac{25\pi^2}{81} \right)^2, & \text{otherwise}, 
\end{cases}
\] (2.18)

where \( c_1 \) is a parameter to control the penalty level induced. It can be shown that \( \psi(\cdot) \) is continuously differentiable and its derivative \( \phi(z) \), called the action function, is given by:

\[
\phi(z) = \begin{cases} 
0, & \text{if } |z| \leq \frac{5\pi}{9}; \\
4c_1 z \left( z^2 - \frac{25\pi^2}{81} \right), & \text{otherwise}.
\end{cases}
\]

### 2.3.3.2 Cyber Control Matrix B

The main function of the cyber matrix \( B \) is to ensure that the effective singular perturbation parameter \( \epsilon = \frac{M_{\text{max}}}{D_{\text{min}} \left( 1 - \sum_{j=1, j \neq i}^{N} b_{ij} \right)} \in \mathcal{O}(0.1) \), where \( M_{\text{max}} \) is the maximum value of \( \{M_i\} \), \( D_{\text{min}} \) is the minimum value of \( \{D_i\} \), \( b_{ij} \) is the \( ij \)th element of \( B \), and typically \( M_{\text{max}}/D_{\text{min}} \in \mathcal{O}(10) \) for practical generators. Also, since \( \Psi = I + B \) has the trivial eigenvalue 1 with corresponding eigenvector \( 1 \), the design of the cyber control matrix \( B \) has the additional constraint:

\[
b_{ii} = - \sum_{j=1, j \neq i}^{N} b_{ij} \in \mathcal{O}(100).
\]

Therefore, we assign the elements of \( B \) as follows:

\[
b_{ij} = \begin{cases} 
c_3, & \text{if } i = j; \\
-\frac{c_1}{N-1}, & \text{otherwise},
\end{cases}
\] (2.19)

where \( c_3 \geq 100 \) is a positive constant.

### 2.3.3.3 Cyber Control Matrix G

Based on Eqs. (2.13), (2.15), and (2.16), we get that the effective Laplacian matrix \( \tilde{L} \) can be described as follows (and incorporates both cyber and physical interactions):

\[
\tilde{L} = M^{-1} (L + G),
\] (2.20)
where \( \mathbf{L} \) is predetermined by the physical power system, \( \mathbf{G} \) is designed by our proposed control protocol, and \( \mathcal{M} \) is determined by the design of \( \mathbf{B} \).

In order to guarantee the frequency convergence of the multiple agents, the Laplacian matrix \( \mathbf{L} \) must be positive semi-definite (PSD), i.e. all its nonzero eigenvalues are located in the right half plane. Therefore, in our control protocol, \( \mathbf{G} \) is designed to achieve a PSD matrix \( \mathbf{\tilde{L}} \). Since \( \mathbf{L} \) and \( \mathbf{G} \) both have the trivial eigenvalue 0 with associated eigenvector \( \mathbf{1} \) (i.e., \( \mathbf{L} \cdot \mathbf{1} = 0 \) and \( \mathbf{G} \cdot \mathbf{1} = 0 \)), we deduce: \( \mathbf{\tilde{L}} \cdot \mathbf{1} = \mathcal{M}^{-1} (\mathbf{L} + \mathbf{G}) \cdot \mathbf{1} = \mathcal{M}^{-1} (\mathbf{L} \cdot \mathbf{1} + \mathbf{G} \cdot \mathbf{1}) = 0 \). Thus the elements of \( \mathbf{\tilde{L}} \) have a rowsum of zero expressed also as:

\[
\tilde{l}_{ii} = - \sum_{j=1, j \neq i}^{N} \tilde{l}_{ij}.
\]  

(2.21)

From Gershgorin’s Theorem [126], we reason that the eigenvalues of \( \mathbf{\tilde{L}} \) are located in the union of the \( N \) discs:

\[
\bigcup_{i=1}^{N} \left\{ z \in \mathbb{C} : \left| z - \tilde{l}_{ii} \right| \leq \sum_{j=1, j \neq i}^{N} |\tilde{l}_{ij}| \right\}.
\]  

(2.22)

Using Eqs. (2.21) and (2.22) we obtain that:

\[
\bigcup_{i=1}^{N} \left\{ z \in \mathbb{C} : \left| z + \sum_{j=1, j \neq i}^{N} \tilde{l}_{ij} \right| \leq \sum_{j=1, j \neq i}^{N} |\tilde{l}_{ij}| \right\}.
\]  

(2.23)

From Eq. (2.23), we deduce that a sufficient condition to ensure \( \mathbf{\tilde{L}} \) is PSD is \( \tilde{l}_{ij} < 0 \) where \( i \neq j \). Therefore, in our control protocol, \( \mathbf{G} \) is designed to achieve a matrix \( \mathbf{\tilde{L}} \) with only negative off-diagonal elements. Letting \( \mathbf{\hat{L}} = \mathbf{L} + \mathbf{G} \) and \( \mathbf{S} = \Psi^{-1} \), we can rewrite Eq. (2.20) as:

\[
\mathbf{\hat{L}} = \mathbf{S} \mathbf{D} \mathbf{\hat{L}}.
\]

Thus, we have that:

\[
\tilde{l}_{ij} = \sum_{k=1}^{N} \frac{s_{ik} \hat{l}_{kj}}{D_k},
\]

where \( \tilde{l}_{ij} \), \( s_{ik} \), and \( \hat{l}_{kj} \) are the elements of the matrices \( \mathbf{\tilde{L}}, \mathbf{S}, \) and \( \mathbf{\hat{L}} \), respectively.

It can be shown that if a matrix is row stochastic and has only non-positive off-diagonal elements, then its inverse matrix is a row stochastic nonnegative matrix; we do not include
the proof in the thesis. Based on this, we have that $S = \Psi^{-1}$ is a row stochastic nonnegative matrix. Therefore $0 \leq s_{ik} \leq 1$ for all $i, k \in 1, 2, \ldots, N$ and $D = 1/\left(\sum_{k=1}^{N} D_k^{-1}\right)$ is a positive constant. Thus, $D\tilde{l}_{ij}$ is a weighted average of the elements on the $j$th column of $\tilde{L}$. We can deduce that as long as $G$ is designed to realize that at least one negative element in each column of $\tilde{L}$, it can be guaranteed that $\tilde{L}$ is PSD as analyzed above.

In order to simplify the controller design, we assume that the cyber communication graph is undirected which (coupled with the fact that the Kron-reduced physical graph is undirected) implies that the integrated cyber-physical graph is undirected thus constraining $\tilde{L}$ to be symmetric. For symmetric Laplacians the convergence rate of consensus is determined by the second smallest eigenvalue. In order to guarantee the convergence rate of the multi-agents’ frequencies and reduce the computational complexity, we design the matrix $G$ to achieve that all the off-diagonal elements of the matrix $\tilde{L}$ to be bounded by a negative upper bound $\rho$. To tradeoff cost of the power transmission $P_u$ and the convergence rate of the frequencies, we choose $\rho \in [-1, -0.5]$.

### 2.3.3.4 Linear Navigation

To reduce the control complexity, we assign the following linear navigation feedback term:

$$F(\omega, \omega_r) = -c_2 (\omega - \omega_r),$$

where $c_2$ is the navigational feedback parameter chosen as 1 in our work, $\omega_r = 0$ denotes the normalized reference frequency.

### 2.3.3.5 Control Signal Design

Based on the above analysis, we have the following result:

$$\dot{u} = -\Gamma - B\omega \cdot \mathbf{D} - c_2 (\omega - \omega_r),$$

(2.24)

where $D = [D_1, \ldots, D_N]^T$. By integrating the both sides of Eq. (2.24), we can formulate $u$, which represents the power transmission $P_u$ between the fast-reacting power source and the synchronized generators, as:

$$u = -\Gamma - \tilde{L}\theta + \eta - B\omega \cdot \mathbf{D} - c_2 (\theta - \theta_0),$$
where the $C$-dimension column vectors $\Gamma = \int_{t_0}^{t} \Phi d\tau$ and $\eta = \int_{t_0}^{t} L \omega d\tau$, and

$$\Gamma(i) = \sum_{j=1,j\neq i}^{N} \int_{t_0}^{t} \phi(\theta_i - \theta_j) d\tau,$$

$$\eta(i) = \sum_{j=1,j\neq i}^{N} \int_{t_0}^{t} P_{ij} \cos(\theta_i - \theta_j + \varphi_{ij}) d\tau = \sum_{j=1,j\neq i}^{N} P_{ij} \sin(\theta_i - \theta_j + \varphi_{ij}),$$

t_0$ is the time to activate our control protocol, and $\theta_0$ is the constant term in $\int_{t_0}^{t} \omega dt$.

### 2.3.4 Stability Analysis of the Proposed Control Protocol

Since our cyber-physical modeling framework aims to address the transient stability problem in smart grid systems, we analyze the controller dynamics in order to deduce its ability to provide regulation in the presence of disruption. We clarify that the practical constraints of the ESS’s power output $P_{u,i} = u_i$ are not included in the stability analysis in this section. However, the case studies in Section 2.5 illustrate that our proposed control protocol is robust to the practical constraints of the ESS’s power output. We emphasize that the control $u_i$ enables a framework to model large-scale distributed cyber-control for transient stability. Moreover, it can provide essential insights into the design of distributed control in future power systems beyond the scope of this thesis.

Letting $\hat{u} = M\hat{\omega}$, we rewrite the dynamics described in Eq. (2.15) as follows:

$$
\begin{cases}
\dot{\theta} = \omega, \\
M \dot{\omega} = \hat{u}.
\end{cases}
$$

where

$$\hat{u} = -\nabla V - (L + G) \omega - c_2 \omega.$$

In order to analyze the stability of our proposed framework, we define the following Lyapunov function $H$:

$$H = \frac{1}{2} \omega^T M \omega + V. \tag{2.25}$$

It is clear that $H(0, 0) = 0$ and $H(\theta, \omega) > 0$ for $\forall (\theta, \omega) \neq (0, 0)$. By calculating the
derivative of $H$ along the dynamics derived in Eq. (2.13), we obtain:

$$
\dot{H} = \omega^T M \dot{\omega} + \omega^T \nabla V,
$$

$$
= \omega^T \dot{u} + \omega^T (-\dot{u} - L \omega - G \omega - c_2 \omega),
$$

$$
= -\omega^T (L + G + c_2 I) \omega. \tag{2.26}
$$

Based on our proposed framework, $\hat{L} = L + G$ is the effective Laplacian matrix which is Positive Definite (PD) and $c_2 > 0$. Therefore, $L + G + c_2 I$ is a PD matrix. Using the property of PD matrices, we deduce $\omega^T (L + G + c_2 I) \omega > 0$. Thus, $\dot{H} < 0$ in Eq. (2.26) demonstrating Lyapunov stability of the proposed framework.

## 2.4 Robustness Analysis with the Communication Delay

### 2.4.1 Communication Delay in Wide Area Power Systems

The proposed flocking-based approach improves Critical Clearance Time (CCT) for maintaining smart grid stability in the face of severe physical fault. This is achieved through the effective integration of PMU data and real-time distributed control. Questions naturally arise as to the overall system performance when the cyber network undergoes natural or intentional delay. In this work we assert that the inherent robustness of flocking behavior provides a natural fortitude against communication delay. We measure this strength by determining a necessary and sufficient condition for smart grid stability that relates both cyber and physical system characteristics.

In our framework the local control $u_i$ for agent $i$ provides an active force to maintain equilibrium in the face of a physical disturbance. To be effective $u_i$ must be responsive to the physical system’s needs for smart grid stability. Bottlenecks in PMU information, detain the computation of $u_i$ raising questions as to acceptable delays in $u_i$ that we study next.

As introduced in [127], the total communication delay $\tau$ for Wide Area Monitoring System (WAMS) can be described as follows:

$$
\tau = \tau_t + \tau_p + \frac{\xi}{R} + \rho_r, \tag{2.27}
$$

where $\tau_t$ is the fixed delay associated with transducers used, DFT processing, data concentration and multiplexing of PMUs, $\tau_p$ denotes the propagation delay, $\xi$ represents the amount of data transmitted, $R$ is the data rate, and $\rho_r$ is the associated random delay jitter.

In our algorithm we assume that PMU information from the various generators are all
buffered and distributed, for example, through a data concentrator such that a consistent delay \( \tau \) is experienced on all cyber data. In the remainder of the section, we denote vectors of delayed information elements with a subscript \( \tau \). The reader should note that delays only occur on information elements. Thus for our delay model, only cyber dynamics exhibit such delays while physical couplings do not display any such latency.

2.4.2 Delay Analysis

In this section we derive a cyber-physical relationship that guarantees robustness of our flocking-based control paradigm to cyber delay. Let \( \hat{u} = M\tilde{u} \). Assuming a communications delay of \( \tau \), our proposed control protocol can be represented as follows:

\[
\begin{align*}
M\dot{\omega} &= \hat{u}, \\
\hat{u} &= -\nabla V_{\tau} - L\omega - G_{\tau}\omega_{\tau} - c_2 (\omega_{\tau} - \omega_r)
\end{align*}
\]  

(2.28)

where \( \omega_r = 0 \), \( V_{\tau} \) and \( G_{\tau} \) represent the potential function and the consensus-based cyber coupling matrix obtained based on the delayed states of the phase angles, respectively, and \( \omega_{\tau} \) is the column vector representing the delayed states of the generator frequencies.

Let \( \varepsilon = \theta - \theta_{\tau} = \int_{-\tau}^0 \omega(t + \eta)d\eta \). Since each element of \( \omega \) is bounded, it follows that for \( \tau \ll 1, \varepsilon \ll 1 \). Moreover, since \( V_{\tau} \) and \( G_{\tau} \) are both dependent on \( \theta \) alone, we can approximate them via \( V \) and \( G \), respectively. Based on the above analysis, we can rewrite Eq. (2.28) as:

\[
\begin{align*}
M\dot{\omega} &= \hat{u}, \\
\hat{u} &= -\nabla V - L\omega - G\omega_{\tau} - c_2 \omega_{\tau}.
\end{align*}
\]  

(2.29)

To analyze the effect of delay on the stability of our framework, we define the following Lyapunov function \( H_{\tau} \):

\[
H_{\tau} = \frac{1}{2} \omega^T M\omega + V + \int_{-\tau}^0 \omega^T(t + \eta)Q\omega(t + \eta)d\eta
\]  

(2.30)

where \( Q \) is a positive semi-definite (PSD) matrix. We can show \( H(0, 0) = 0 \) and \( H(\theta, \omega) > 0 \) for \( \forall (\theta, \omega) \neq (0, 0) \).
By calculating the derivative of $H$ along the dynamics derived in Eq. (2.29), we obtain:

$$
\dot{H}_\tau = \omega^T M \dot{\omega} + \omega^T \nabla V + \omega^T Q \omega - \omega^T_r Q \omega_r,
$$

$$
= \omega^T \dot{u} + \omega^T (-\dot{u} - L \omega - G \omega_r - c_2 \omega_r) 
+ \omega^T Q \omega - \omega^T_r Q \omega_r,
$$

$$
= \omega^T (-L \omega - G \omega_r - c_2 \omega_r) + \omega^T Q \omega - \omega^T_r Q \omega_r,
$$

(2.31)

By defining

$$
m = \omega - \omega_r = \int_{-\tau}^0 \dot{\omega}(t + \eta) d\eta,
$$

(2.32)

we can rewrite Eq. (2.31) as follows:

$$
\dot{H}_\tau = -\omega^T (L + G - Q) \omega + \omega^T G m - c_2 \omega^T \omega_r - \omega^T_r Q \omega_r,
$$

$$
= -\omega^T (L + G - Q) \omega - \omega^T_r (Q + c_2 I) \omega_r 
- \omega^T_r (c_2 I - G) m + m^T G m.
$$

(2.33)

Letting $Q = L + G = \hat{L}$, we obtain:

$$
\dot{H}_\tau = -\omega^T_r (\hat{L} + c_2 I) \omega_r - \omega^T_r (c_2 I - G) m + m^T G m.
$$

(2.34)

Based on Eq. (2.19), we observe that $\hat{L} + c_2 I$ is positive definite (PD). Since we design the cyber coupling matrix $G$ to ensure $\hat{L} = L + G$ is PD, based on Proposition 8.1.2 viii) of [128], $G$ is also PD. Through eigendecomposition we have the following result:

$$
c_2 I - G = U \Lambda_1 U^{-1},
$$

(2.35)

where $\Lambda_1 = \text{diag}(\lambda_1, \ldots, \lambda_N)$ and $\lambda_i$ is the $i$th eigenvalue of $c_2 I - G$. Thus, using Proposition 9.1.6 in [128] we obtain:

$$
-\omega^T_r (c_2 I - G) m \leq \mu \|\omega_r\| \|m\|,
$$

(2.36)

where $\mu = \max\{|\lambda_1|, \ldots, |\lambda_N|\}$. 

Since \( \tilde{L} + c_2 I \) is a PD symmetric matrix, based on Lemma 8.4.3 in [128] we have:

\[
-\omega_r^T \left( \tilde{L} + c_2 I \right) \omega_r \leq -\lambda_n \| \omega_r \|^2,
\]

where \( \lambda_n \) is the minimum eigenvalue of \( \tilde{L} + c_2 I \) and \( \| \cdot \| \) denotes the 2-norm of the vector. Since in our framework, \( \tilde{L} \) is a Laplacian matrix whose minimum eigenvalue is 0, we obtain that \( \lambda_n = c_2 \). Thus, we rewrite Eq. (2.37) as follows:

\[
-\omega_r^T \left( \tilde{L} + c_2 I \right) \omega_r \leq -c_2 \| \omega_r \|^2.
\]

Since \( G \) is PD, using eigendecomposition and Proposition 8.1.2 xiii) of [128], we have:

\[
m^T G m \leq \lambda_m \| m \|^2,
\]

where \( \lambda_m \) is the maximum eigenvalue of the matrix \( G \).

By using Eqs. (2.34), (2.36), (2.38), and (2.39), we achieve an upper bound of \( \dot{H}_r \) as follows:

\[
\dot{H}_r = -\omega_r^T \left( \tilde{L} + c_2 I \right) \omega_r - \omega_r^T (c_2 I - G) m + m^T G m,
\]

\[
\leq -c_2 \| \omega_r \|^2 + \mu \| \omega_r \| \| m \| + \lambda_m \| m \|^2,
\]

where \( c_2 > 0, \mu \geq 0, \lambda_m > 0 \), \( \| \omega_r \| \) and \( \| m \| \) are both nonnegative and independent of each other, and the value of \( \| m \| \) is dependent on the extent of the time delay \( \tau \) as shown in Eq. (2.32).

Based on the property of quadratic functions and the fact that \( \| \omega_r \| \) is nonnegative, we have that \( \dot{H}_r < 0 \) if and only if the following relationship between \( \| m \| \) and \( \| \omega_r \| \) is satisfied:

\[
\| m \| < \frac{2c_2}{\mu + \sqrt{\mu^2 + 4c_2 \lambda_m}} \| \omega_r \|,
\]

where \( m \) is the difference between \( \omega \) and \( \omega_r \), \( c_2 \) is our designable cyber control parameter, \( \lambda_m \) is the maximum eigenvalue of our designed cyber control matrix \( G \), and \( \mu \) is the maximum eigenvalue of \( c_2 I - G \). Eq. (2.41) therefore reveals that the robustness of our proposed flocking-based framework can be successfully tuned through proper selection of control parameter \( c_2 \) and the control matrix \( G \). We next demonstrate the controller performance in the presence of delay empirically.
2.5 Simulations and Performance Assessment

Tests are conducted on the WECC 3-Generator Power System of Fig. 2.5 for the 3-phase short circuit faults on two locations. The generator parameters are given in Table 2.1.

![Image](image_url)

Figure 2.5: WECC 3-Generator power system.

Table 2.1: Generator Parameters for WECC 3-Generator Power System

<table>
<thead>
<tr>
<th>Generator No.</th>
<th>H pu</th>
<th>$X'_{d}$ pu</th>
<th>E pu</th>
<th>Angle (rad)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10</td>
<td>0.08</td>
<td>1.04</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>3.01</td>
<td>0.18</td>
<td>1.02</td>
<td>-3.55</td>
</tr>
<tr>
<td>3</td>
<td>6.4</td>
<td>0.12</td>
<td>1.05</td>
<td>-2.9</td>
</tr>
</tbody>
</table>

To enable modeling of a wide area power system, the normalized line impedances typically set to $0.1j$ are increased to $0.35j$ reducing the physical generator couplings thus making the problem of achieving smart grid stability more difficult. DSATools™ is employed for simulations. In each case we assume that a physical fault occurs at time $t = 0$ s and the associated line is removed after the associated Critical Clearing Time (CCT) of value. Then, the control is activated 3 cycles (i.e. 0.05 s) after the fault is cleared, in which the parameters $c_1$, $c_2$, $c_3$ are set to $1/20$, 1 and 1, respectively. The distributed controllers determine $u_i = P_{u,i}$ as detailed in the previous section and may undergo information processing delays.

2.5.1 Case Study I

In the first study, a 3-phase short circuit is applied to the middle of Line 4-5 and has corresponding CCT 0.05 s. Fig. 2.6 presents the rotor frequencies and phase angle differences over a period of 6.5 s when the fault is cleared at 0.15 s (after the CCT) and no control is applied. Instability is clearly evident in all plots. Fig. 2.7 demonstrates performance when the fault is
once again cleared at 0.15 s but this time our proposed flocking-based control is applied at \( t = 0.2 \) s. We assume that the ESSs employed in our simulation are able to provide up to 100 MW of power for short time duration, which means that the power transmission limit for each fast-acting ESS is set to \( P_{u,i} \leq 1 \) p.u. The advanced energy storage techniques make this assumption achievable. For instance, the Nickel-Cadmium Battery in Fairbanks, Alaska can provide 40 MW power for 7 mins [129], and thus the ESSs required in our control protocol can be realized by using multiple Nickel-Cadmium Battery of this type simultaneously. The power transmission \( P_u = (P_{u,1}, P_{u,2}, P_{u,3}) \) is shown in Fig. 2.8. Even though clipping of the control signal occurs, smart grid stability is still achieved.

In order to evaluate the performance of the proposed flocking-based control protocol, we include the generator governor for simulating the dynamical behavior of the power system. The block diagram of governor control system employed in our simulation is illustrated in Fig. 2.9.
in which the parameters for each generator’s governor control system is set as: \( R = 0.05 \), \( T_1 = 0.5 \), \( T_2 = 0.3 \), \( T_3 = 2 \), \( D_t = 0 \), \( V_{MIN} = 0 \), and \( P_{MAX} = 9.99 \text{ p.u.} \).

In order to evaluate the performance of the governor control system by assigning the parameters as above, we consider a situation when the fault is cleared at \( t = 4 \) cycles (i.e. 0.0667 s). Figs. 2.10 and 2.11 present the rotor frequencies and phase angle differences with and without considering the dynamics of governor control system in Fig. 2.9, respectively.

From Figs. 2.10 and 2.11, we observe that the governor control system employed in our simulation helps to improve the phase angle stability and frequency stability of the WECC 3-Generator Power System and is able to restabilize the power system when the fault is cleared right after the CCT. We continue to study the impact of the governor control system on the performance of our proposed flocking-based control protocol. We take into account the dynamics of the governor control system for the original situation in this case study, in which the fault is cleared at \( t = 0.15 \) s and the proposed control protocol is applied at time \( t = 0.2 \) s. Figure 2.12 presents the rotor frequencies and phase angle differences over a period of 10 s and Fig. 2.13 shows the power output of each ESS. Compared with the simulation results in Figs. 2.7 and 2.8, we can obtain that the performance of our proposed control protocol in smart grid sta-
Figure 2.10: (a) The normalized frequencies and (b) the rotor phase angle differences versus time without considering the dynamics of governor control system.

Figure 2.11: (a) The normalized frequencies and (b) the rotor phase angle differences versus time by considering the dynamics of governor control system.
bility maintenance is improved by taking account of governor control systems. Therefore, if the proposed flocking-based control protocol can successfully restabilize the system without taking into account the governor control systems, we can always conclude that our control protocol can efficiently maintain the smart grid stability when the governor control systems are considered.

Figure 2.12: (a) The normalized frequencies and (b) the rotor phase angle differences versus time with flocking-based control and governor control systems.

Figure 2.13: Power transmission $P_u$ between the generators and the fast-acting ESSs in the presence of our proposed protocol and governor control systems.

Figures 2.14 and 2.15 validate and illustrate that our proposed approach is also robust to the communication delay. We set this delay to $\tau = 0.1$ s using the same simulation parameters as for Fig. 2.7.

2.5.2 Case Study II

In the next study, Bus 6 is shorted and then cleared at 0.3 s (after the CCT of 0.2 s). Figures 2.16 and 2.17 present the rotor frequencies, phase angles and phase angle differences
Figure 2.14: (a) The normalized frequencies and (b) the rotor phase angle differences versus time with flocking-based control under the communication delay $\tau = 0.1$ s.

Figure 2.15: (a) The normalized frequencies and (b) the rotor phase angle differences versus time with flocking-based control and governor control systems under the communication delay $\tau = 0.1$ s.
when no control is applied. Figure 2.17 takes into account the dynamics of governor control system which is shown in 2.9, while Figure 2.16 does not consider the governor control systems. Instability is observed in both cases. Furthermore, by comparing Figs 2.16 and 2.17 we can also observe the function of governor control system on improving the frequency stability and phase angle stability.

![Figure 2.16](image1)

**Figure 2.16:** (a) The normalized frequencies and (b) the rotor phase angle differences versus time with neither control nor governor control systems.

![Figure 2.17](image2)

**Figure 2.17:** (a) The normalized frequencies and (b) the rotor phase angle differences versus time without control.

Figures 2.18 and 2.19 illustrate the performance of our proposed flocking-based control without and with considering the governor control systems. In both situations, the power transmission limit for each fast-acting ESS is set to $P_{u,i} \leq 1$. The power transmission $P_u = (P_{u,1}, P_{u,2}, P_{u,3})$ in these two situations is shown in Fig. 2.20. By observing Figs. 2.18 to 2.20, we can get that even though clipping of the control signal occurs smart grid stability is still achieved in both situations. Furthermore, the performance of our proposed control protocol is better when taking into account the governor control systems. Figures 2.21 and 2.22 validate and demonstrate that our proposed secure is robust to a communication delay of $\tau = 0.1$ s.
Figure 2.18: (a) The normalized frequencies and (b) the rotor phase angle differences versus time with flocking-based control.

Figure 2.19: (a) The normalized frequencies and (b) the rotor phase angle differences versus time with flocking-based control and governor control systems.

Figure 2.20: Power transmission $P_u$ between the generators and the fast-acting ESSs in the presence of our proposed protocol (a) [left] without considering governor control systems, (b) [right] considering governor control systems.
Figure 2.21: (a) The normalized frequencies and (b) the rotor phase angle differences versus time with flocking-based control under the communication delay $\tau = 0.1$ s.

Figure 2.22: (a) The normalized frequencies and (b) the rotor phase angle differences versus time with flocking-based control and governor control systems under the communication delay $\tau = 0.1$ s.
2.6 Conclusions

We have investigated a multi-agent dynamical system framework for modeling cyber-physical smart grid interactions related to the smart grid stability problem. Each agent consists of a synchronous power generator, PMU and local controller. Access to a fast-acting power grid enables application of power control for smart grid stability. The physical system operation is described through the application of swing equations to a kron-reduced power network. The cyber system operation, which includes communications and control tasks, is integrated with the physical through a flocking control paradigm. We have demonstrated the elegant way in which cyber and physical couplings are described in the dynamical system equations of each agent. Furthermore, we study the performance of our approach to information delay both analytically and empirically to demonstrate the robustness of our control strategy in the face of incidental or intentional information disruptions. The simulations show the potential of the approach for modeling and providing insights on distributed smart grid strategies for smart grid stability.
Chapter 3

Two-Tier Hierarchical Cyber-Physical Security Framework

3.1 Introduction

The effective modeling of a power grid can significantly improve the understanding of its operation and design. In this chapter, we consider a dynamical systems-based cyber-physical representation that aims to provide power system designers with insights on how to leverage distributed control to maintain transient stability in the face of significant disruptions. Recent work has just begun to address this problem. In [130], Ilić et al. propose a dynamic framework to represent the interactions amongst generators and loads. Here a module with linear closed-loop dynamics is used to represent each generator and load that are interconnected using a linear network model of the system. In [131], Li and Han study how the addition of communication links can effectively re-stabilize a faulted power grid. They employ a linearized swing equation-based model relating the overall generator synchronization to spectral properties of a matrix that is a weighted sum of the Laplacian of the (physical) power graph and the (cyber) communication network. A greedy search algorithm is proposed to identify a communication topology that can enable synchronism for a given smart grid topology. The work introduced in Chapter 2 has studied the analogy between the dynamics of generator synchronization and that of flocking theory. A distributed cyber-physical control approach is developed such that in the face of disturbances, the system is re-stabilized by “steering” its dynamics as a cohesive flock.

Given the value of this flocking metaphor, in this chapter we extend our work introduced in Chapter 2 and make the following contributions. First, we formally explore how information and physical couplings can be synergistically harnessed for re-stabilizing a power grid under severe attack or fault. Through analysis we assess how hierarchy and the selective use of cy-
ber information can benefit scalability and robustness to information attack. Second, through a flocking-based paradigm we develop distributed control methodologies that leverage cooperation between distributed energy resources (DERs) and traditional synchronous machines to maintain transient stability in the face of severe disturbances. Third, we introduce and apply the notion of state-dependent hierarchy in which coherent generator clusters from disturbance are leveraged such that strong physical couplings are identified to selectively apply distributed cyber-control where necessary. Fourth, based on the proposed hierarchical cyber-physical security analysis framework, we consider a cyber-physical viewpoint to the problem of data corruption in smart grid systems. We take the perspective that one may leverage natural physical couplings amongst power system components as telltale signs to identify information corruption and demonstrate how cyber corruption can be identified within the power system by taking a hierarchical cyber-physical perspective. Specifically, the physical coherence within the second tier of a two-tier cyber-physical structure is probed to execute a “witness”-based cyber-physical protocol to identify and mitigate cyber attack in first tier.

3.2 Two-Tier Hierarchical Cyber-Physical Control Protocol

3.2.1 Hierarchical Cyber-Physical Dynamics

We model the cyber-physical integration in the smart grid with a two-tier hierarchical multi-agent framework shown in Fig. 3.1. Each agent consists of both cyber and physical elements: (1) a dynamic node representing a physical power system element, in this case a generator, (2) a phasor measurement unit (PMU) that acquires generator phase angle and frequency data from the dynamic node, and (3) a local cyber-controller that computes a control signal that is applied to the agent’s generator using PMU data. Each agent’s frequency, phase angle, and coherency characteristics are those of its generator. The PMU and local controller are both considered to be cyber elements due to their data acquisition, communication and computation tasks. The physical coherency between active agents is timely achieved by using our real-time dynamic coherency identification method which will introduced in Section 3.5. The agents with high physical coherency are considered to form a cluster and one agent within the cluster (typically with highest generator inertia) is selected as the lead agent.

We illustrate the implementation of the hierarchical control framework for the well-known New England 39-bus system in Fig. 3.2. Here, we assume there are three clusters and the lead agent of each cluster is denoted with a shaded (green) generator. Effective PMU information (cyber) and power (physical) flows are presented as dashed and solid arrows, respectively. To further delineate the tiered nature of communications, red, blue and magenta dashed arrows
represent tiered communications from lowest to highest level. Therefore, only the lead agent’s PMU and local cyber-control are activated for overall cluster regulation and the phasor data concentrator (PDC) in each cluster is implemented to guarantee synchronization of the data information flows amongst lead agents. Therefore, this enables a state-dependent system hierarchy whereby inter-cluster interactions are cyber-physical (tier-1) and intra-cluster synergies are physical (tier-2).

3.2.2 Hierarchical Control Protocol Design by Analogy to Flocking

3.2.2.1 Dynamic Description of Cyber-Physical Integration

The hierarchical control protocol is developed based on the flocking-based dynamical systems paradigm introduced in Chapter 2. In this hierarchical framework, the cyber network (PMU data + local controllers) is integrated into this framework through controlling the fast-acting EES power absorption/injection, $P_{u,i}$, to Generator Bus $i$ to compensate for fluctuations in demand power in the system after a severe disturbance. Letting the control signal $u_i = P_{u,i}$ and $\alpha_i$ be a binary number defined as follows:

$$\alpha_i = \begin{cases} 1, & \text{if the } i\text{th agent is the lead agent;} \\ 0, & \text{otherwise,} \end{cases} \quad (3.1)$$
we can formulate the dynamics of our cyber-physical integrated framework as follows:

\[
M_i \ddot{\omega}_i = -D_i \omega_i + P_{m,i} - E_i^2 G_{ii} - \sum_{j=1, j \neq i}^{N} P_{ij} \sin \left( \theta_i - \theta_j + \phi_{ij} \right) + \alpha_i u_i. \tag{3.2}
\]

where physical inter-agent couplings (denoted \(\text{phys} \)) are characterized by parameters \(P_{ij}\) and \(\phi_{ij}\) and cyber couplings (\(\text{cyber} \)) through \(u_i\). For normal operation \(u_i = 0\). However, when a disturbance strikes, \(u_i\) will excite the system to re-achieve (smart grid) stability.

We design the control signal \(u_i\) under two assumptions. First, we assume that, in the face of severe disturbance, \(u_i = P_{u,i}\) changes much faster than the mechanical power input \(P_{m,i}\) for each agent and the time span to recover smart grid stability is short; thus we treat \(P_{m,i}\) as a constant during the procedure of maintaining smart grid stability. This assumption is reasonable for future smart grids where fast-response energy storage such as battery storage and flywheels will be available to inject and absorb energy for periods of brief control. Second, we assume that the problems of voltage regulation and frequency synchronization are decoupled. This enables us to consider the voltage \(E_i\) as a constant during controller excitation to re-achieve the frequency synchronization.

Under these assumptions, computing derivatives of the both sides of Eq. (3.2), and refor-
where the index assignments are reordered such that Agents $i = 1, \ldots, C$ correspond to lead agents, $C$ is the number of clusters in our hierarchical framework, $\alpha = \text{diag}[\alpha_1, \ldots, \alpha_N]$, $\alpha_i = 1$ for $i \leq C$, and $\alpha_i = 0$ otherwise. $\theta = [\theta_1, \ldots, \theta_N]^T$, $\omega = [\omega_1, \ldots, \omega_N]^T$, $u = [u_1, \ldots, u_N]^T$, $M = \text{diag}[M_1, \ldots, M_N]$, $D = \text{diag}[D_1, \ldots, D_N]$, and $L$ is a $N \times N$ physical coupling matrix whose elements can be represented as:

$$l_{ij} = \begin{cases} \sum_{j=1, j \neq i}^N P_{ij} \cos (\theta_i - \theta_j + \varphi_{ij}), & \text{if } i = j; \\ -P_{ij} \cos (\theta_i - \theta_j + \varphi_{ij}), & \text{if } i \neq j, \end{cases}$$

(3.4)

### 3.2.2.2 Hierarchical Cyber-Physical Dynamics

In our hierarchical framework, the agents are grouped into the same cluster if they have high physical coherency, and we assert that the deviations between the states (i.e. phase angle and normalized relative frequency) of the secondary agents and their lead agents are very small. Therefore, we propose to treat the states $(\theta_i, \omega_i)$ of Secondary Agent $i$ as “noisy” versions of those of Lead Agent $k$ which is in its cluster and estimate $(\theta_i, \omega_i)$ as follows:

$$\begin{cases} \hat{\omega}_i = \omega_k + \Delta_i \\ \hat{\theta}_i = \theta_k + \varepsilon_0^i + \varsigma_i \end{cases}$$

(3.5)

where $\varepsilon_0^i$ denotes the phase angle difference between the $i$th and $k$th agents in the static (pre-fault) state, and $\Delta_i \sim \mathcal{U} (-a, a)$ and $\varsigma_i \sim \mathcal{U} (-b, b)$ are uniform random noises on $[-a, a]$ and $[-b, b]$, respectively, with $a \ll 1$ and $b \ll 1$.

By using Eq. (3.5), we are able to estimate the information of the physical coupling matrix $L$ by only using the lead agents’ states. To simplify, we partition $L$ as follows:

$$L = \begin{bmatrix} R_{C \times C} & S_{C \times (N-C)} \\ T_{(N-C) \times C} & U_{C \times C} \end{bmatrix}.$$ 

By using Eq. (3.5), we can approximate the matrix $S$ with $\hat{S}$ whose element is shown as follows:

$$\hat{S}(j, k) = -P_{jk} \cos (\theta_j - \theta_k - \varepsilon_0^j + \varphi_{jk}),$$

(3.6)

where the $i$th secondary agent belongs to the $k$th cluster. Using Eq. (3.6), we can approximate
the matrix $R$ by using $\hat{R}$ whose element is defined as follows:

$$\hat{R}(i,j) = \begin{cases} R(i,j), & \text{if } i \neq j; \\ -\sum_{j=1, j \neq i}^{C} R(i,j) - \sum_{j=C+1}^{N} \hat{S}(i,j), & \text{otherwise.} \end{cases} \quad (3.7)$$

Based on Eqs. (3.6), (3.7), (3.3), and (3.5), we achieve the hierarchical cyber-physical dynamics as follows:

1. **The lead agents (tier-1):**

   $$\begin{cases} \dot{\theta}_l = \omega_l, \\ D_l\dot{\omega}_l = -M_l\ddot{\omega}_l - (\hat{R} + \hat{S}\Psi)\omega_l + \dot{u}_l - \hat{S}\Delta, \end{cases} \quad (3.8)$$

   where the subscript, $\omega_l = [\omega_1, \ldots, \omega_C]^T$, $\theta_l = [\theta_1, \ldots, \theta_C]^T$, $D_l = \text{diag}[D_1, \ldots, D_C]$, $M_l = \text{diag}[M_1, \ldots, M_C]$, $u_l = [u_1, \ldots, u_C]^T$, $\Delta = [\Delta_{C+1}, \ldots, \Delta_N]^T$, 

   $$\Psi(i,j) = \begin{cases} 1, & \text{if the } (C + i)\text{th agent is in the } j\text{th cluster;} \\ 0, & \text{otherwise.} \end{cases}$$

2. **The secondary agents (tier-2):**

   $$\begin{cases} \dot{\theta}_s = \omega_s, \\ D_s\dot{\omega}_s = -L_s\omega_s - M_s\dot{\omega}_s, \end{cases} \quad (3.9)$$

   where $L_s$ denotes the physical coupling matrix for secondary agents, $M_s = \text{diag}[M_{C+1}, \ldots, M_N]$, $\theta_s = [\theta_{C+1}, \ldots, \theta_N]^T$, and $\omega_s = [\omega_{C+1}, \ldots, \omega_N]^T$. Because the associated local controllers and ESSs are not activated for the secondary agents, their dynamics as described in Eq. (3.9) is equivalent to the dynamics represented in Eq. (2.7).

### 3.2.2.3 Design by Analogy to Flocking

In Chapter 2, we have proposed the flocking-inspired control assignment providing smart grid stability for non-hierarchical cyber-physical framework. In this section, we propose a two-tier hierarchical control framework which leverage the physical coherency between the agents and only apply the flocking-inspired assignment on the lead agents. As shown in the next section, we prove that given an accurate identification of generator coherency, the following flocking-based distributed cyber-physical control law modeled guarantees smart grid stability.

$$\dot{u}_l = -\Phi + (\hat{R} + \hat{S}\Psi)\omega_l - L\omega_l - c_2 (\omega_l - \omega_r) - B\dot{\omega}_l. \quad (3.10)$$
where $\mathbf{B}$ is a pre-designed $C \times C$ cyber coupling diagonal matrix whose diagonal element $B_i \geq (100 \times D_i)$, $c_2$ is a positive parameter for the linear navigational feedback, $\omega_r = 0$ is the desired relative normalized generator frequency, $\Phi = \nabla V(\theta_l)$ is the gradient of $V(\theta_l)$ with respect to $\theta$, $V(\theta_l)$ represents the potential energy function to guarantee that the phase angle difference between each pair of lead agents is bounded, which is defined as follows:

$$V(\theta_l) = \frac{1}{2} \sum_{i=1}^{C} \sum_{j=1, j \neq i}^{C} \chi(\theta_i - \theta_j),$$

where $\chi(\cdot)$ is a pairwise attractive potential defined in Eq. (2.18). Therefore, the gradient $\Phi$ can be represented as follows:

$$\Phi(i) = \sum_{j=1, j \neq i}^{C} \phi(\theta_i - \theta_j),$$

$$\phi(z) = \begin{cases} 0, & \text{if } |z| \leq \frac{5\pi}{9}; \\ 4c_1 z \left(z^2 - \frac{25\pi^2}{81}\right), & \text{otherwise}. \end{cases}$$

and $\mathbf{L}$ is another $C \times C$ cyber coupling matrix designed to achieve frequency consensus and its $ij$th element is set as:

$$L_{ij} = \begin{cases} c_3, & \text{if } i = j; \\ \frac{c_i}{C-1}, & \text{otherwise}. \end{cases}$$

Based on Eqs. (3.8) and (3.10) and $\omega_r = 0$, we can reformulate the cyber-physical dynamics of the lead agents as follows:

$$\begin{align*}
\dot{\theta}_l &= \omega_l, \\
(D_l + B) \ddot{\omega}_l &= -M_l \ddot{\omega}_l - \Phi - L_l \omega_l - c_2 \omega_l - S \Delta, 
\end{align*}$$

which represents a linear second-order differential equation with respect to $\omega_l$. In practice, for the $i$th synchronized generator, the ratio between the inertia $M_i$ and the damping parameter $D_i$ satisfies $M_i/D_i \in \mathcal{O}(10)$ [117]. We therefore find that the associated perturbation parameter for Lead Agent $i$ is $\epsilon_i = M_i / (D_i + B_i) \in \mathcal{O}(0.1)$ representing an overdamped system, which enables the application of singular perturbation techniques to in Eq. (3.14) to study the dynamics of the lead agents over a longer time scale. Specifically, applying singular perturbation
analysis and letting \( M = D_l + B_l \) [125] gives:

\[
\begin{cases}
\dot{\theta}_l = \omega_l, \\
M \dot{\omega}_l = -\Phi - L \omega_l - c_2 \omega_l - S \Delta.
\end{cases}
\]  

(3.15)

Here, the simplification has allowed the physical notion of generator “jerk” related to \( \ddot{\omega}_l \) to be eliminated from the dynamics.

By integrating both sides of Eq. (3.10), we can formulate \( u_l \), which represents the power transmission \( P_u \) between the fast-reacting power source and the synchronized generators, as:

\[
u_l = -\Gamma + \int_{t_0}^{t} \left( R + S \right) \omega_l d\tau - L \theta_l - c_2 \theta_l - B \omega_l,
\]

(3.16)

where \( \theta_0 \) is the constant term in \( \int_{t_0}^{t} \omega d\tau \) and \( \Gamma = \int_{t_0}^{t} \Phi d\tau \) whose element is represented as follows:

\[
\Gamma(i) = \sum_{j=1,j\neq i}^{C} \left[ \int_{t_0}^{t} \phi (\theta_i - \theta_j) d\tau \right].
\]

(3.17)

Let the \( C \)-dimension column vector \( \eta \) denote \( \int_{t_0}^{t} \left( R + S \right) \omega_l d\tau \). Since \( \hat{R} \), \( \hat{S} \), and \( \Phi \) are time-varying and their information is available, using (3.4) and (3.6) we obtain:

\[
\eta(i) = \sum_{j=1,j\neq i}^{C} P_{ij} \sin (\theta_{ij} + \varphi_{ij}) + \sum_{j=1,j\neq i}^{C} \sum_{k \in \mathcal{I}_j} P_{ik} \sin (\theta_{ij} - \varepsilon_k^0 + \varphi_{ik}) - \eta_i^0,
\]

where \( \mathcal{I}_j \) denotes the index set of the secondary agents belonging to the \( j \)th cluster, \( \omega_{ij} = \omega_i - \omega_j \), \( \theta_{ij} = \theta_i - \theta_j \), and

\[
\eta_i^0 = \left[ \sum_{j=1,j\neq i}^{C} P_{ij} \sin (\theta_{ij} + \varphi_{ij}) + \sum_{j=1,j\neq i}^{C} \sum_{k \in \mathcal{I}_j} P_{ik} \sin (\theta_{ij} - \varepsilon_k^0 + \varphi_{ik}) \right]_{t=t_0}.
\]

### 3.2.3 Hierarchical Control Protocol Stability Analysis

We define the following Lyapunov function \( H \):

\[
H = \frac{1}{2} \omega_l^T \Phi \omega_l + V(\theta_l)
\]

(3.18)
for which \( H(0, 0) = 0 \) and \( H(\theta, \omega) > 0 \) for \( \forall (\theta, \omega) \neq (0, 0) \). Calculating the derivative of \( H \) along the dynamics derived in Eq. (3.15) we obtain:

\[
\dot{H} = \omega_i^T \mathcal{M} \dot{\omega} + \omega_i^T \nabla V(\theta) = \omega_i^T \mathcal{M} \dot{\omega} + \omega_i^T \Phi. \tag{3.19}
\]

Based on Eq. (3.15), we have the followings:

\[
\Phi = -\mathcal{M} \dot{\omega} - \tilde{\mathcal{L}} \omega - c_2 \omega - \tilde{S} \Delta. \tag{3.20}
\]

By substituting Eq. (3.20) to Eq. (3.19), we have:

\[
\dot{H} = -\omega_i^T \left( \tilde{\mathcal{L}} + c_2 \mathbf{I} \right) \omega - \omega_i^T \tilde{S} \Delta. \tag{3.21}
\]

Based on our proposed framework, \( \tilde{\mathcal{L}} \) is the effective Laplacian matrix which is PSD and \( c_2 > 0 \). Therefore, \( \left( \tilde{\mathcal{L}} + c_2 \mathbf{I} \right) \) is a Positive Definite (PD) matrix, and thus \( \omega_i^T \left( \tilde{\mathcal{L}} + c_2 \mathbf{I} \right) \omega > 0 \).

Since information on \( \omega \) and \( \tilde{S} \) is available and \( \tilde{\mathcal{L}} \) and \( c_2 \) are designable, using Lyapunov redesign method, we obtain:

\[
\dot{H} \leq -\lambda_m \| \omega \|^2 + \rho \| \omega \| \| \tilde{S} \| = -\| \omega \| \left( \lambda_m \| \omega \| - \rho \| \tilde{S} \| \right) \tag{3.22}
\]

where \( \lambda_m \) is the smallest eigenvalue of \( \left( \tilde{\mathcal{L}} + c_2 \mathbf{I} \right) \).

Since \( \tilde{\mathcal{L}} \) is a Laplacian with minimum eigenvalue 0, \( \lambda_m = c_2 \). Therefore, \( \dot{H} < 0 \) is guaranteed when the following condition is satisfied:

\[
\| \omega \| \geq \frac{\rho}{c_2} \| \tilde{S} \|. \tag{3.23}
\]

The high physical coherency between intra-cluster agents ensures that \( \rho \) is sufficiently small. In practice, the tolerance interval of the normalized relative frequency is \([-0.02, 0.02]\), and thus \( \rho < 0.02 \). Therefore, we can design \( c_3 \) to satisfy:

\[
c_2 \geq \frac{\rho \| \tilde{S} \|}{0.02}. \tag{3.24}
\]

Based on Eqs. (3.23) and (3.24), we deduce that \( \dot{H} < 0 \) if \( \| \omega_i \| > 0.02 \), where \( i = 1, 2, \ldots, C \). Thus, the frequencies of all the lead agents are bounded within the required tolerance interval \([-0.02, 0.02]\). Thus, our proposed distributed control guarantees smart grid stability given the existence of an accurate and efficient coherent cluster identification algorithm.
CHAPTER 3. TWO-TIER HIERARCHICAL CYBER-PHYSICAL SECURITY FRAMEWORK 54

3.3 Multi-Flock-Based Timely Coherency Generator Identification Method

This section presents a timely dynamic technique for generator coherency identification, Multi-Flock-Based Coherency Identification Method. Generator coherency identification is establishing itself as an important task to aid in the resistance of cascading failures within wide-area power systems and as a necessary pre-processing stage in real-time control for transient stability. Efficient generator coherency identification is critical to ensure the success of the hierarchical cyber-physical control framework proposed in Section 3.2.

3.3.1 Literature Review

As we shift towards an era of “smarter” power systems, we witness increased functionality and scale due to load growth and generation expansion. Physical components, increasingly operated under stress in this newly deregulated market, exhibit protracted inter-area oscillations detrimental to the goals of maximizing system stability and optimizing power transfer [132].

Wide-Area Monitoring, Protection And Control (WAMPAC) systems are designed to address the problem of inter-area oscillation. A necessary first step in this process is to first identify the nature of the oscillatory behavior.

Inter-area oscillations are a complex phenomenon observed between interconnected synchronous generators in power systems. These oscillations, associated with groups of generators that swing against each other at frequencies below 1 Hz, are intrinsically nonlinear and dynamic [133]. Generator coherency is used to characterize the observation that generators naturally form clusters, following a disturbance such that generators angles within the same coherent group oscillate faster with respect to one another than those in distinct groups [134].

Much research has been done to analyze inter-area oscillation and to identify generator coherency arising from this phenomenon [133–141]. Classical techniques can be categorized into three types. The first class identifies generator coherency by analyzing the empirical results of offline simulation [134, 135]; such approaches exhibits high accuracy but are inappropriate for addressing disturbances dynamically in real-time. The second type employs linearized power system models about the power flow equilibrium to reduce complexity [136], but is often unsuitable to represent large or rapid deviations from the equilibrium. The third class introduces the notion of slow coherency arising from inter-area oscillations [137]. These methods use singular perturbation to assess time-scale separation of the inter-area and local modes, and implement eigenvector-based methods to identify coherent generator groups. One disadvantage is the inefficiency of these methods when the inter-area oscillation is not sufficiently reduced.
Furthermore, all three classes require detailed power system topology data, which may not always be available when needed especially for emerging wide area smart grid systems.

To address this problem, measurement-based coherency identification employing phasor measurement units (PMUs) has been proposed. PMUs provide real-time synchronized phasor information of quantities including voltage and current at generator and load busses. PMUs have been developed to measure generator rotor frequencies and phase angles to an accuracy of 0.2% [142–144]. Based on such capabilities, the authors of [138] propose a short-time Fourier transform (STFT)-based coherency identification method applied to generator frequency measurements. Here, the Fourier coefficient with largest magnitude is used to identify the dominant inter-area mode. A sufficiently long observation window is critical for performance hence making it inappropriate when only a short duration of data exists upon which to make decisions. The methods proposed in [140, 141] somewhat relax the window length requirement. In [140], the authors employ Koopman modes (KM) derived through spectral analysis of the Koopman operator, a linear operator defined to analyze nonlinear dynamical systems. KM analysis is applied on generator frequency data to characterize nonlinear oscillatory modes for coherency identification. The author in [141] applies the Hilbert-Huang transform on generator phase angle data to identify coherency.

3.3.2 Problem Setting

In this section we aim to detect generator coherency by proposing an analogy between the coherency of generators and the interactions among flockmates in multiple flocks. We extend a single flocking paradigm to include the characterization of multiple species flocking via a feature similarity rule. Here, a flock flockmate aims to stay close to those flockmates representing similar coherency indices and stays apart from flockmates with dissimilar features much like the flock separation observed for different species in nature.

We assert that a flocking paradigm exhibits the following advantages. The robustness of the flocking process to perturbation and sudden environmental change would make a clustering algorithm based on this analogy more robust to measurement noise and data corruption. Furthermore, the representation of generator data as directed trajectories of flockmate dynamics enables opportune assessment of future movement and imminent clustering. We emphasize that this predictive quality reduces the need for advanced computation and dramatically decreases the observation time window in contrast to existing techniques.

Our coherency identification technique makes use of a transformation from the observation space to an information space where decisions on generator coherence are directly made. The bulk of our proposed technique involves the mapping from these domains and is detailed in
Section 3.3.3.

Figure 3.3: (a) New England 39-bus power system, (b) Flocking-based analogy where flockmates travel through information space.

Figure 3.4: Traveling flockmates’ directed trajectory in the information space.

As illustrated in Figs. 3.3 and 3.4, for the New England 39-bus power system, each flockmate in the flocking scenario embodies the state information of a corresponding generator of the power system. For \( C \) generators indexed as \( i = 1, 2, \ldots, C \), Flockmate \( i \) embodies the information of Generator \( i \). In nature, flockmates of the same species are within the same flock. In our technique, the species feature of each Flockmate \( i \) is determined by the information describing Generator \( i \)’s status in the observation space and is defined as

\[
\begin{align*}
\mathcal{I}_i^1(k) &= \theta_i(k) \\
\mathcal{I}_i^2(k) &= \omega_i(k) \\
\mathcal{I}_i^3(k) &= \delta_i(k)
\end{align*}
\]

(3.25)

where \( \mathcal{I}_i(k) = [\mathcal{I}_i^1(k) \ \mathcal{I}_i^2(k) \ \mathcal{I}_i^3(k)]^T \), \( \theta_i(k) \) and \( \omega_i(k) \) are the phase angle and the normalized frequency, respectively, of the \( i \)th generator at the time step \( t = k \) that are obtained directly
from PMU information, and \( \dot{\delta}_i(k) \) is the acceleration of the \( i \)th generator at the time step \( t = k \) estimated from the current and historical values of \( \omega_i(k) \) as we later discuss.

In the information space, we describe the dynamic state of each flockmate as
\[
S_i(k) = [p_i(k), v_i(k)]^T,
\]
where \( p_i(k) \) denotes Flockmate \( i \)’s position initialized randomly, and \( v_i(k) \) is Flockmate \( i \)’s velocity initialized to 0. We also consider two flockmates to be neighbors at time step \( t = k \) if the distance between them is less than the predetermined threshold \( d_c \), and thus define the index set of neighbors for the \( i \)th flockmate as follows:
\[
N_i(k) = \{ \forall j \neq i \mid \|p_i(k) - p_j(k)\| < d_c \},
\]
which is comprised of the indices of all of Flockmate \( i \)’s neighbors.

The flockmate positions are initialized to random locations. Then, each new generator data set in the observation space affects the movement of its associated flockmate in the observation space as shown in Fig. 3.4. Despite its initial values, we assert based on empirical experience that, over time, the flockmates’ relative positions and velocities converge to invariant clusters through the interaction with neighboring flockmates. The flockmates assemble into multiple flocks, largely determined by their species feature that must be appropriately defined such that groups within the configuration correspond to generator clusters.

For example, by observing Fig. 3.4, we can conclude that Flockmates 2 and 3 are in the same flock and Flockmates 3 to 10 constitute another flock, which indicates a generator coherency following a serious fault of \( \{G_1\}, \{G_2, G_3\}, \) and \( \{G_4, G_5, \ldots, G_{10}\} \).

### 3.3.3 Multi-Flock-Based Generator Coherency Identification

We assume that each generator has a phasor measurement unit (PMU) that acquires its phase and frequency information and communicates with a control center [138, 145]. To identify generator coherency using our approach, the control center would map the generator frequency and phase to flockmate dynamics in the information space and then analyze the interactions between these flockmates. The corresponding generator frequency and phase information of a flockmate relative to that of another neighboring flockmate represents a feature, which in turn determines the nature of its interaction with its neighbor. Let \( \chi_{ij}^k = p_j(k) - p_i(k) \) be the Euclidean displacement between the Flockmate \( i \) and \( j \) in the information space at time \( t = k \).

We consider the flockmates’ interaction at each time step \( t = k \) to be characterized in terms of a weighted combination of intra-flock interaction and inter-flock interaction modeled through the use of a potential function \( V^k(\chi_{ij}^k) \), which is a function of variable \( \chi_{ij}^k \) and defined as:
\[
V^k(\chi_{ij}^k) = \sum_{l=1}^{3} w_l V_l^k(\chi_{ij}^k),
\] (3.26)
where $V_i^k$ models the intra-flock centering and collision avoidance, $V_2^k$ represents the intra-flock velocity matching, and $V_3^k$ is used to account for inter-flock obstacle avoidance. Thus, the relative similarity in state of a pair of generators is employed to produce a potential between the corresponding flockmates via $V^k$, which imposes accelerations on the flockmates to determine the flockmates’ pairwise interactions and trajectories. The acceleration caused by a force Flockmate $j$ imposes on Flockmate $i$ is computed by differentiating the potential function $V^k$ with respect to the relative position vector between Flockmate $i$ and $j$. Thus, the overall acceleration of Flockmate $i$ would be a vector sum of the individual accelerations caused by each of Flockmate $i$’s neighbors.

### 3.3.3.1 Multi-Flock Modeling

#### 3.3.3.1.1 Feature Similarity

The potential functions can be computed for a pair of neighboring flockmates only after the feature similarity is calculated. We compute a species feature similarity between neighboring flockmates as follows. For $j \in \mathcal{N}_i(k)$, the indices of all Flockmate $i$ neighbors,

$$
\zeta_{ij}(k) = \sum_{n=1}^{3} \alpha_n (I^n_i(k) - I^n_j(k)),
$$

where $\{\alpha_n\}$ is a positive scalar weight influencing the impact of information class $n$ on flockmate interaction. As evident, $\zeta_{ij}(k)$ is smaller for higher feature similarity.

Based on Eq. (3.27), we calculate a dynamic threshold $\zeta_{th}(k)$ and determine whether a pair of neighboring flockmates are part of the same flock by comparing their feature similarity with this threshold value; the procedure is detailed in Table 3.1. First, we define set $\zeta(k)$, which is a collection of the feature similarities between all the pairwise neighboring flockmates at time $t = k$, and then obtain a sorted row vector $\tilde{\zeta}_k$ consisting of the the $C$ smallest elements of $\zeta(k)$ in ascending order. Second, we select the first $N_s$ smallest feature similarity values (i.e., the first $N_s$ elements of $\tilde{\zeta}_k$) to compute the dynamic threshold $\zeta_{th}(k)$ via a weighted summation of the maximum and the mean of the smallest $N_s$ feature similarity values. Finally, we conclude that Flockmates $i$ and $j$ have high similarity if the sign of $s_{ij}(k) = \zeta_{ij}(k) - \zeta_{th}(k) \leq 0$. The reader should note that the value of $s_{ij}(k)$ will be employed to compute each potential function for a pair of neighbors.

#### 3.3.3.1.2 Intra-Flock Centering and Collision Avoidance

Intra-flock centering and collision avoidance involves the attraction of flockmates to one another such that they are in the same geographic proximity but are non-colliding. We model this for flockmates within the
Table 3.1: Neighboring Flockmate Relationships.

At time \( t = k \),
1. For neighboring Flockmates \( i \) and \( j \), calculate \( \zeta_{ij}(k) \) using Eq. (3.27) and construct set \( \zeta(k) = \{ \zeta_{ij}(k) | i = 1, \ldots, C, \text{ and } j \in \mathcal{N}_i(k) \} \).
2. Form the \( 1 \times C \) row vector \( \zeta_k \) by populating it with the \( C \) smallest values of \( \zeta(k) \) sorted in ascending order.
3. Calculate the dynamic threshold as follows:
   \[ \zeta_{th}(k) = w_s \zeta_k(N_s) + \frac{1}{N_s} \zeta_k \text{l,} \]
   where \( 0 < w_s < 1 \), \( 0 < N_s \leq C \) is used to determines the collection of \( \zeta_{ij}(k) \) used to calculate the threshold, and \( \text{l} \) is a \( C \)-dimensional column vector and defined as follows:
   \[ l(k) = \begin{cases} 1, & \text{if } k \leq N_s; \\ 0, & \text{otherwise.} \end{cases} \]
4. If \( s_{ij}(k) = \zeta_{ij}(k) - \zeta_{th}(k) \leq 0 \), they are considered to exhibit feature similarity. Otherwise, they are considered to be dissimilar.

same flock through inter-flockmate forces that depend on relative displacement and informational similarity. Thus, for \( s_{ij}(k) \leq 0 \), Flockmates \( i \) and \( j \) are assumed to exhibit cohesion; they are attracted to one another up to a desired position distance \( d^* \) (at which point we consider the attraction strength to decrease to zero) and then if any closer, slightly repel each other to avoid collision. The higher informational similarity between the flockmates, the stronger (weaker) the strength (repulsion) when their distance is above (below) \( d^* \).

We design a nonnegative potential energy function \( V_{1i}^k(\chi_{ij}^k) \) for all \((i, j)\) such that \( j \in \mathcal{N}_i(k) \) and \( s_{ij}(k) \leq 0 \), which reaches its minimum only when its argument \( \chi_{ij}^k \) implies a position separation between Flockmates \( i \) and \( j \) of distance \( d^* \):

\[
V_{1i}^k(\chi_{ij}^k) = \sum_{i=1}^{C} \sum_{j \in \mathcal{N}_i(k)} \left\{ \frac{\gamma_1}{\gamma_2} \cdot \exp \left[ \frac{\gamma_2 s_{ij}(k)(\|\chi_{ij}^k\|_\sigma - \|d^*\|_\sigma)}{\|\chi_{ij}^k\|_\sigma - \|d^*\|_\sigma} \right] - \gamma_1 s_{ij}(k) \left( \|\chi_{ij}^k\|_\sigma - \|d^*\|_\sigma \right) \right\},
\]

(3.28)

where \( \gamma_1 \) and \( \gamma_2 \) are positive parameters, and \( \|\cdot\|_\sigma \) denotes the \( \sigma \)-norm \( \|\chi\|_\sigma = \frac{1}{\epsilon} \left( \sqrt{1 + \epsilon \|\chi\|} - 1 \right) \) which is used to guarantee the potential energy function \( V_{1i}^k(\chi_{ij}^k) \) is always differentiable, especially when \( \chi_{ij}^k = 0 \). If \( s_{ij}(k) > 0 \) then \( V_{1i}^k(\chi_{ij}^k) = 0 \).

Using Eq. (4.12), we calculate the corresponding action function \( g_{1i,j}^k(k) \), which is equivalent to the acceleration caused by the potential energy function \( V_{1i}^k \), by differentiating \( V_{1i}^k \) with
respect to relative displacement $\chi_{ij}^k$ [146] to give:

$$g_{i,j}^1(k) = \nabla \chi_{ij}^k V_1^k(\chi_{ij}^k)$$

$$= \frac{\gamma_1 \cdot s_{ij}(k) \cdot (\chi_{ij}^k)}{\sqrt{1 + \epsilon \|\chi_{ij}^k\|^2}} \left\{ \exp \left[ \gamma_2 s_{ij}(k) \|\chi_{ij}^k\|_\sigma - \|d^\sigma\|_\sigma \right] - 1 \right\}$$  \hspace{1cm} (3.29)

for all $(i, j)$ such that $j \in N_i(k)$ and $s_{ij}(k) \leq 0$ and $g_{i,j}^1(k) = 0$ otherwise.

### 3.3.3.1.3 Velocity Matching

In a flock, flockmates typically demonstrate alignment of their velocities. It is well established that this can be modeled as a distributed consensus problem in which the flockmates represent the vertices of a dynamic graph and the associated edge weights determine the degree of interaction to achieve alignment [123]. Letting $A$ be the dynamic graph’s associated adjacency matrix with elements $a_{ij}(k)$, we design the following potential energy function for all $(i, j)$ such that $j \in N_i(k)$ and $s_{ij}(k) \leq 0$:

$$V_2^k(\chi_{ij}^k) = (\chi_{ij}^k)^T L \chi_{ij}^k,$$  \hspace{1cm} (3.30)

where $L$ is the graph’s associated Laplacian matrix: $L = \Delta (A) - A$ and $\Delta A$ is a diagonal matrix with the $i$th diagonal element as $\sum_{j=1}^n a_{ij}(k)$. For $s_{ij}(k) > 0$, $V_2^k(\chi_{ij}^k) = 0$.

In our framework, the interaction that achieves alignment is designed to be constant when the relative displacement $\chi_{ij}^k$ is below the threshold $d_c$ (i.e., $j \in N_i(k)$) and reduces to $0$ otherwise. Therefore, we assign the adjacency matrix elements of such a graph in our formulation as:

$$a_{ij}(k) = \rho_h \left( \|\chi_{ij}^k\|_\sigma / \|d_c\|_\sigma \right),$$  \hspace{1cm} (3.31)

for $j \in N_i(k)$ where $h \in [0, 1)$ is a parameter, and

$$\rho_h(x) = \begin{cases} 
1, & x \in [0, h]; \\
\frac{1}{2} \left[ 1 + \cos \left( \pi \left( x - h \right) / (1 - h) \right) \right], & x \in [h, 1]; \\
0, & \text{otherwise}.
\end{cases}$$

Using Eqs. (3.30) and (3.31), we determine the corresponding acceleration to be:

$$g_{i,j}^2(k) = a_{ij}(k) \, \chi_{ij}^k$$  \hspace{1cm} (3.32)

for all $(i, j)$ such that $j \in N_i(k)$ and $s_{ij}(k) \leq 0$ and $g_{i,j}^2(k) = 0$ otherwise, as desired.
3.3.3.1.4 **Obstacle Avoidance** For $s_{ij}(k) = \zeta_{ij}(k) - \zeta_{th}(k) > 0$, Flockmates $i$ and $j$ are considered to exhibit low feature similarity. Their interaction is modeled as a mutual avoidance in which each considers the other to be an obstacle in their flock’s trajectory. We model the corresponding repulsion strength to be dependent on their degree of dissimilarity and their relative distance to one another; the higher the dissimilarity the stronger the repulsion up to a distance threshold $d_r$ at which point their repulsion strength decreases to 0. Thus, we design the following potential energy function for all $(i, j)$ such that $j \in \mathcal{N}_i(k)$ and $s_{ij}(k) > 0$:

$$V^k_3(\chi^k_{ij}) = \begin{cases} \
\frac{\gamma_3}{2} \sum_{i=1}^{C} \sum_{j \in \mathcal{N}_i(k)} s_{ij}(k) \left( \| \chi^k_{ij} \|_{\sigma} - \| d_r \|_{\sigma} \right)^2, & \text{if } \| \chi^k_{ij} \| \leq d_r; \\
0, & \text{otherwise.} 
\end{cases}$$

where $\gamma_3$ is a positive parameter. $V^k_3(\chi^k_{ij}) = 0$ for $s_{ij}(k) \leq 0$.

We calculate the acceleration caused by $V^k_3$ as:

$$g^3_{i,j}(k) = \nabla_{\chi^k_{ij}} V^k_3(\chi^k_{ij}) = \gamma_3 s_{ij}(k) \left( \| \chi^k_{ij} \|_{\sigma} - \| d_r \|_{\sigma} \right)$$

for all $(i, j)$ such that $j \in \mathcal{N}_i(k)$ and $s_{ij}(k) \leq 0$ and $g^3_{i,j}(k) = 0$ otherwise.

### 3.3.3.2 Coherent Generator Identification

To ensure that the flockmates’ trajectories are always within the field of view, in our framework the interaction between the flockmates only affects the direction, rather than magnitude of the flockmates’ velocity. Thus each active flockmate traveling in the information space has a velocity with constant magnitude and varying direction. Furthermore, the continuity of the generators’ measurements in the observation space and the flockmates’ movement in the information space indicate a continuous nature of the interaction amongst the traveling flockmates. Therefore, the interaction at current time step $t = k$ can be predicted by the value at the previous time step $t = k - 1$ with certain prediction accuracy $w_p$. Based on this fact, we improve the robustness of our technique to potential measurement noise and cyber attack by accounting for the consistency in the nature of interaction at the current time step $t = k$ with the previous time instant $t = k - 1$. Specifically, if the signs of $s_{ij}(k - 1)$ and $s_{ij}(k)$ are consistent, the flockmate’s acceleration is calculated based on the interaction achieved at $t = k$, otherwise, the flockmate’s acceleration is calculated based on two components: the first component is related to the interaction achieved at $t = k$ (based on the observation data at this current time step) and the second component is the predicted interaction based on the trajectory set at $t = k - 1$. 
These components are weighted via the prediction accuracy parameter $w_p$. The resulting model of Flockmate $i$ dynamics is detailed in Table 3.2.

The state of each flockmate $S_i(k) = [p_i(k), v_i(k)]^T$ is used to plot its trajectory in time during the observation period. From this graph, we can easily obtain the grouped arrangement of the flockmates indicating coherent clusters of generators. To better elucidate our technique, we summarize variables in Table 3.3 and list parameters in Table 3.5. In the next section we demonstrate how our technique effectively determines coherent generator clusters under a variety of faults.

3.3.4 Case Studies

We evaluate the effectiveness of our generator coherency identification technique by using the New England 39-Bus test system detailed in [1] consisting of $C = 10$ generators whose parameters are shown in Table 3.4. MATLAB/Simulink is employed for simulations. The average computation time of our proposed method is $0.11$ s using an AMD FX(tm)-8320 Eight-Core Processor and 16 GB RAM. This can be dramatically reduced with dedicated and more advanced processors.

In this section, we consider three situations representing an ideal environment, one with white noise, and one with false data injection. In each situation, we employ PMUs with sampling frequency of 50 Hz and set the observation window length to $T = 100$ ms, which is selected empirically through trial and error for different test faults, and $T = 500$ ms, which is used to evaluate the performances of different techniques. The reader should note that it was found through tests on the IEEE 9-bus, IEEE 14-bus and New England 39-Bus test systems that the observation window length depends on the test system’s complexity and PMU sampling rate. Specifically, higher complexity systems and PMU sampling rates below 50 Hz generally require longer observation windows.

In each case, we initialize the positions of the flockmates randomly in the information space for each trial and run 10 independent trials. We conclude the generator coherency determination based on the dominant conclusion of the flockmate groupings amongst the 10 trials. To assess the performance of our approach, we compare our technique with the classical modal analysis-based scheme by Chow [137] as well as two measurement-based methods proposed in [138] and [140]. The parameters are selected empirically under ideal conditions and are listed in Table 3.5.
Table 3.2: Flockmate Dynamics.

Let $s_{ij}(k - 1) = \zeta_{ij}(k - 1) - \zeta_{th}(k - 1)$ for $k \geq 1$ and $g^l_{ij}(k)$ be acceleration calculated by using Eqs. (4.13), (4.14), and (4.16). Compute $\hat{f}_{ij}(k)$, to quantify the interactions between neighboring Flockmates $i$ and $j$, as follows.

At time $t = k$,
1. for $j = 1 : C$
   if $j \neq i$
     if $k = 0$
     
     $$\hat{f}_{ij}(k) = \begin{cases} 
     \sum_{l=1}^{2} w_l g^l_{ij}(k), & \text{if } s_{ij}(k) \leq 0; \\
     w_3 g^3_{ij}(k), & \text{otherwise.}
\end{cases}$$

     else

     (1). if $s_{ij}(k) \leq 0$ and $s_{ij}(k - 1) \leq 0$:
     $$\hat{f}_{ij}(k) = \sum_{l=1}^{2} w_l g^l_{ij}(k);$$

     (2). if $s_{ij}(k) \leq 0$ and $s_{ij}(k - 1) > 0$:
     $$\hat{f}_{ij}(k) = (1 - w_p) \sum_{l=1}^{2} w_l g^l_{ij}(k) + w_p w_3 g^3_{ij}(k - 1);$$

     (3). if $s_{ij}(k) > 0$ and $s_{ij}(k - 1) > 0$:
     $$\hat{f}_{ij}(k) = w_3 g^3_{ij}(k);$$

     (4). otherwise:
     $$\hat{f}_{ij}(k) = w_p \sum_{l=1}^{2} w_l g^l_{ij}(k - 1) + (1 - w_p) w_3 g^3_{ij}(k);$$

     where $0 < w_p < 0.5$ determines impact of the historical information on the current decision.

2. Calculate the dynamics of Flockmate $i$ at time $t = k + 1$ as follows:

$$\begin{cases}
    v_i(k + 1) = v_i(k) + \Delta t \sum_{j=1, j \neq i}^{C} \hat{f}_{ij}(k), \\
    v_i(k + 1) = \rho_v v_i(k + 1) / \|v_i(k + 1)\|, \\
    p_i(k + 1) = p_i(k) + \Delta t v_i(k),
\end{cases}$$

where $\Delta t$ is the time step for coherence identification and $\rho_v > 0$ represents the constant magnitude of each flockmate’s velocity.
Table 3.3: Main Variables Used in Proposed Approach

<table>
<thead>
<tr>
<th>$I_i$</th>
<th>$\theta_i$</th>
<th>$\omega_i$</th>
<th>$\delta_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flockmate $i$'s carried information</td>
<td>Generator $i$'s phase angle</td>
<td>Generator $i$'s frequency</td>
<td>Generator $i$'s acceleration</td>
</tr>
<tr>
<td>$S_i$</td>
<td>$p_i$</td>
<td>$v_i$</td>
<td>$\zeta_{ij}$</td>
</tr>
<tr>
<td>State of Flockmate $i$</td>
<td>Position of Flockmate $i$</td>
<td>Velocity of Flockmate $i$</td>
<td>Feature similarity between Flockmates $i$ and $j$</td>
</tr>
<tr>
<td>$s_{ij}$</td>
<td>$\mathcal{N}_i$</td>
<td>$\chi_{ij}$</td>
<td>$g_i^j$</td>
</tr>
<tr>
<td>Relative feature similarity with respective to threshold $\chi_{th}$</td>
<td>Index collection of Flockmate $i$'s neighbors</td>
<td>Distance between Flockmates $i$ and $j$</td>
<td>Acceleration of Flockmate $i$ caused by interaction with Flockmate $j$ based on $V_i$</td>
</tr>
</tbody>
</table>

3.3.4.1 Ideal Environment

In this section, we consider the situation in which the PMU measurements used for the generator coherency determination have high accuracy.

3.3.4.1.1 Case 1  We assume a three-phase fault to occur immediately outside Bus 21 on Line 21 − 22 at $t = 0$. The associated Line 21 − 22 is opened at $t = 100$ ms. The generators’ normalized rotor frequencies and phase angles over a period of 5 s are shown in Fig. 3.5. We observe that the generator coherency involving the following groups: $\{G_1\}$, $\{G_6, G_7\}$, and $\{G_2, G_3, G_4, G_5, G_8, G_9, G_{10}\}$.

![Normalized rotor frequencies and phase angles versus time of 10 s.](image)

Since the transient stability maintenance is time-critical, there is only a brief observation period to determine the generator coherency. Fig. 3.6 shows the flockmate trajectories for the ob-
CHAPTER 3. TWO-TIER HIERARCHICAL CYBER-PHYSICAL SECURITY FRAMEWORK

Table 3.4: Generator Parameters and Initial Conditions for New England 39-Bus Power System [1]

<table>
<thead>
<tr>
<th>Generator No.</th>
<th>H pu</th>
<th>$X'_d$ pu</th>
<th>E pu</th>
<th>Angle (rad)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>500</td>
<td>0.006</td>
<td>1.0368</td>
<td>-0.1344</td>
</tr>
<tr>
<td>2</td>
<td>30.3</td>
<td>0.0697</td>
<td>1.1966</td>
<td>0.3407</td>
</tr>
<tr>
<td>3</td>
<td>35.8</td>
<td>0.0531</td>
<td>1.1491</td>
<td>0.3417</td>
</tr>
<tr>
<td>4</td>
<td>38.6</td>
<td>0.0436</td>
<td>1.0808</td>
<td>0.2985</td>
</tr>
<tr>
<td>5</td>
<td>26</td>
<td>0.132</td>
<td>1.3971</td>
<td>0.5088</td>
</tr>
<tr>
<td>6</td>
<td>34.8</td>
<td>0.05</td>
<td>1.191</td>
<td>0.3376</td>
</tr>
<tr>
<td>7</td>
<td>26.4</td>
<td>0.049</td>
<td>1.1394</td>
<td>0.3499</td>
</tr>
<tr>
<td>8</td>
<td>24.3</td>
<td>0.057</td>
<td>1.0709</td>
<td>0.307</td>
</tr>
<tr>
<td>9</td>
<td>34.5</td>
<td>0.057</td>
<td>1.1368</td>
<td>0.5335</td>
</tr>
<tr>
<td>10</td>
<td>42</td>
<td>0.031</td>
<td>1.0929</td>
<td>-0.0087</td>
</tr>
</tbody>
</table>

Table 3.5: Parameters Used in Proposed Approach

<table>
<thead>
<tr>
<th>Parameters used in potential functions</th>
<th>$\gamma_1$</th>
<th>1</th>
<th>Positive weights for flockmates’ carried information</th>
<th>$\alpha_1$</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\gamma_2$</td>
<td>0.5</td>
<td></td>
<td></td>
<td>$\alpha_2$</td>
<td>1</td>
</tr>
<tr>
<td>$\gamma_3$</td>
<td>1/6</td>
<td></td>
<td></td>
<td>$\alpha_3$</td>
<td>3</td>
</tr>
<tr>
<td>Positive weights for potential functions</td>
<td>$w_1$</td>
<td>350</td>
<td>Distance threshold for $V_2$</td>
<td>$d_v$</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>$w_2$</td>
<td>100</td>
<td>Distance threshold for $V_3$</td>
<td>$d_r$</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>$w_3$</td>
<td>750</td>
<td>Desired distance</td>
<td>$d^*$</td>
<td>0.5</td>
</tr>
<tr>
<td>Number of flockmates used to get $\chi_{th}$</td>
<td>$N_s$</td>
<td>10</td>
<td>Parameter used to get $\chi_{th}$</td>
<td>$w_s$</td>
<td>0.6</td>
</tr>
<tr>
<td>Impact of history information</td>
<td>$w_p$</td>
<td>0.2</td>
<td>Normalized magnitude of velocity</td>
<td>$\rho_v$</td>
<td>$10^3$</td>
</tr>
</tbody>
</table>

Observation window length $T = 100$ ms achieved in one trial which achieves the dominant result on flockmate grouping. The arrows on each trajectory indicates the velocity direction of each flockmate. From the trajectories shown in Fig. 3.6, we observe that the flockmates associated with $G_6$ and $G_7$ travel together as well as those associated with $\{G_2, G_3, G_4, G_5, G_8, G_9, G_{10}\}$. Thus, we visually conclude that the flockmates constitute three flocks identifying coherent generator groups.

For consistent comparison, the modal analysis method of [137], the STFT method of [138] and the KM-approach of [140] are first implemented with the same observation time window length of 100 ms and PMU sampling of 50 Hz. The modal analysis method uses singular perturbation analysis to achieve an inter-area oscillation of 0.43 Hz and uses an eigenvector-based algorithm to obtain the slow eigensubspace matrix,

$$
V_s = \begin{bmatrix}
0.32 & 0.32 & 0.32 & 0.32 & 0.32 & 0.32 & 0.32 & 0.32 \\
-0.30 & 0.23 & 0.24 & 0.35 & 0.40 & 0.41 & 0.40 & 0.23 & 0.31 & 0.20
\end{bmatrix},
$$
based on which the coherent groups of generators are incorrectly identified as \( \{ G_1 \} \), and \( \{ G_2, \ldots, G_{10} \} \). However, the reader should note that with a longer observation window of 500 ms, this method computes inter-area oscillations 0.27 Hz and 0.67 Hz and obtains a slow eigensubspace matrix from which coherent groups of generators are correctly identified as \( \{ G_1 \}, \{ G_6, G_7 \}, \) and \( \{ G_2, G_3, G_4, G_5, G_8, G_9, G_{10} \} \). The above simulations show that the modal analysis method achieves accurate identification of generator coherency when the observation time window is long enough such that inter-area oscillations are sufficiently damped. The performance of this method degrades when the observation window is short.

<table>
<thead>
<tr>
<th>Time Window</th>
<th>( G_1 )</th>
<th>( G_2 )</th>
<th>( G_3 )</th>
<th>( G_4 )</th>
<th>( G_5 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 ms</td>
<td>0</td>
<td>-95.61</td>
<td>-67.37</td>
<td>-53.18</td>
<td>-77.75</td>
</tr>
<tr>
<td>500 ms</td>
<td>0</td>
<td>-5.86</td>
<td>-8.91</td>
<td>-27.87</td>
<td>-5.80</td>
</tr>
<tr>
<td>Time Window</td>
<td>( G_6 )</td>
<td>( G_7 )</td>
<td>( G_8 )</td>
<td>( G_9 )</td>
<td>( G_{10} )</td>
</tr>
<tr>
<td>100 ms</td>
<td>20.88</td>
<td>37.67</td>
<td>-51.15</td>
<td>-64.28</td>
<td>-1.51</td>
</tr>
<tr>
<td>500 ms</td>
<td>35.38</td>
<td>20.66</td>
<td>-19.22</td>
<td>-12.52</td>
<td>-26.01</td>
</tr>
</tbody>
</table>

The results of [138] where the relative phases of the largest magnitude non-zero Fourier coefficients of each inter-area mode are computed are shown in Table 3.6. Since the observation window length used here is much less than the window length, 100 s, selected in [138], it is reasonable to obtain the phase angle comparison \( \Delta \varphi_{k,dom} \) at one time index. The phase comparison results in Table 3.6 incorrectly indicates that the generator coherency is \( \{ G_1, G_{10} \} \) \( \{ G_6, G_7 \} \), and \( \{ G_2, G_3, G_4, G_5, G_8, G_9 \} \) with the time window of 100 ms, and correctly as \( \{ G_1 \}, \{ G_6, G_7 \}, \) and \( \{ G_2, G_3, G_4, G_5, G_8, G_9, G_{10} \} \) with time window 500 ms. Thus, the

The KM-based method of [140] is implemented to achieve the domain Koopman Modes by analyzing the generators’ frequency measurement. When the time window is 100 ms, there are two dominant KMs and Fig. 3.7(a) plots the initial phase $\alpha_{ij}$ versus amplitude coefficients $A_{ij}$ of KM $j$ for $G_i$. Based on the distribution of $A_{ij}$ and $\alpha_{ij}$ shown in Fig. 3.7(a), we can identify the generator coherency as $\{G_1, G_6, G_7\}$, and $\{G_2, G_3, G_4, G_5, G_8, G_9\}$, and the grouping for $G_{10}$ is ambiguous. When the time window is 500 ms, there is one dominant KM and the distribution of $A_{ij}$ and $\alpha_{ij}$ is shown Fig. 3.7(b), from which we can correctly conclude the coherent groups of generators as $\{G_1, G_6, G_7\}$, and $\{G_2, G_3, G_4, G_5, G_8, G_9, G_{10}\}$. Thus, the method of [140] also exhibits limited performance for short observation windows.

![Figure 3.7](image)

(a) (b)

Figure 3.7: The distribution of amplitude coefficients $A_{ij}$ and initial phases $\alpha_{ij}$ for the dominant KMs with the observation time windows of (a) 100 ms and (b) 500 ms.

3.3.4.1.2 Case 2 We consider that a three-phase fault occurs in the middle of the Line 14 – 15 at time $t = 0$ s and the fault is cleared at $t = 100$ ms, post-Critical Clearing Time (CCT). The generators’ normalized rotor frequencies and phase angles over a period of 10 s are shown in Fig. 3.8 revealing the following true coherent clusters groups: $\{G_1\}$, $\{G_2, G_3\}$, and $\{G_4, G_5, \ldots, G_{10}\}$. The flockmate trajectories of one trial of our proposed technique achieve the dominant result shown in Fig. 3.20. As evident, the flockmate associated with $G_1$ travels away from the others that form two groups, one corresponding to $G_2$ and $G_3$, and the other to $G_4$ to $G_{10}$.

With the observation time window of 100 ms, the modal analysis method [137] achieves inter-area oscillation $0.42$ Hz and mistakenly identifies the coherent groups of generators as $\{G_1\}$, and $\{G_2, \ldots, G_{10}\}$. With an observation time window of 500 ms, however, this method achieves inter-area oscillations $0.25$ Hz and $0.81$ Hz to correctly identify $\{G_1\}$, $\{G_2, G_3\}$, and $\{G_4, \ldots, G_{10}\}$. Thus, this case also reveals a limitation when the observation window is too
Figure 3.8: (a) Normalized rotor frequencies and (b) phase angles versus time of 10 s.

Figure 3.9: The trajectories of the flockmates with the observation time windows of (a) 100 ms and (b) 500 ms.
For the method of [138] with time window of 100 ms, we calculate the phase angle comparison to incorrectly conclude the result of \( G_1 \), \( G_2, G_3, G_4, G_5, G_6, G_7 \), and \( G_{9, G_{10}} \). For a time window of 500 ms, we obtain \( G_1 \), \( G_2, G_3 \), \( G_4, \ldots, G_8, G_{10} \), and the grouping for \( G_9 \) is ambiguous, since it can be either grouped into the second or third group. For the technique of [140], we plot the distribution of amplitude coefficients and initial phases for the dominant KMs and identify the generator coherency incorrectly as \( G_1 \), \( G_2, \ldots, G_{10} \) for a 100 ms time window. For a time window of 500 ms, we correctly determine the coherency as \( G_1 \), \( G_2, G_3 \), and \( G_4, \ldots, G_{10} \).

These results illustrate that in order to ensure accuracy, the modal analysis-, STFT- and KM-based methods all require sufficiently long observation windows, which may be impractical for emerging smart grid systems that exhibit extremely short time scales before reaction is required.

### 3.3.4.2 Measurement Environment with White Noise

To account for nonidealities, we evaluate the robustness of our proposed generator coherency identification technique to environmental white noise. We consider the same faults on Line 21–22 and Line 14–15 as in Section 3.3.4.1 and an observation window of 100 ms. In each case, we evaluate our performance for various signal-to-noise ratios (SNRs) by running 100 independent trials for each value of SNR. Moreover, we consider the situation that there is white noise on the generators’ phase angle and frequency measurements.

#### 3.3.4.2.1 Fault on Line 21–22

Figure 3.10(a) shows the success rate versus SNR value from 1 to 100. From Fig. 3.10(a), we observe the trade-off between high robustness at the high noise level and the high accuracy at the low noise level in our technique by considering the historical feature and dynamics of the traveling flockmates. When the noise level is relatively low (i.e. \( SNR \geq 10 \) dB), our proposed generator coherency identification technique is more robust to white noise on the measurement of frequency than that of phase angle. When the noise on the measurement of phase angle or frequency has \( SNR \geq 10 \) dB, our proposed technique achieves the percentage of success above 85%. Even when the noise level is very high (i.e. \( SNR = 1 \) dB), our proposed technique is still able to guarantee the percentage of success above 69%.

#### 3.3.4.2.2 Fault on Line 14–15

The success rate versus SNR value from 1 to 100 are, shown in Figure 3.10(b). Here, we observe that by considering the historical feature and dynamics of the traveling flockmates, our proposed technique has the trade-off between high robustness
3.3.4.3 Measurement Environment with False Data Injection

We evaluate the robustness of our technique to the popular false data injection attack on PMU measurements defined as follows.

**Attack Model** The opponent is able to corrupt $P_a$ percentage of the generator bus PMUs by biasing the phase angle readings with error $e_1 = 0.5$ rad and frequency readings with error $e_2 = 1$. We consider the same fault test cases as Section 3.3.4.1 and set the observation time window length as 100 ms.

3.3.4.3.1 Fault on Line 21 – 22 Figure 3.11 (a) shows the success rate versus percentage of PMU being attacked, $P_a$, on phase angle and frequency, respectively. From Fig. 3.11 (a), we observe that the success rate is worst when the attacker attempts to attack 50% PMU readings under the attack model we considered. This is expected because by assuming the same bias on the attacked PMU readings, the relative features between biased readings are maintained. If most of the readings are biased, then their interactions will be the same as when they are not biased. Figure 3.11 (a) also indicates that, in the worst case under the considered attack model, our propose method guarantees the percentage of success above 78% when the PMU phase
angle readings are corrupted and guarantees 79% success when the PMU frequency readings are corrupted.

### 3.3.4.3.2 Fault on Line 14 – 15

Figure 3.11 (b) shows the success rate versus percentage of PMUs being attacked on phase angle and frequency, respectively. From Fig. 3.11 (b), we observe that under the worst situation when 50% PMU readings are attacked, our proposed method guarantees the percentage of success above 72% when the phase angle PMU readings are attacked and guarantees success above 75% when the frequency PMU readings are corrupted.

Thus the above studies illustrate that our proposed measurement-based technique is robust to false data injection. Such resilience stems from our use of an information space that models generator dynamics via flocking interactions. Such interactions are tolerant to false data injection, which constitutes an interruption of the corrupted dynamics. Thus our approach is able to mitigate the impact of false data injection more successfully.

![Figure 3.11: The percentage of success versus percentage of PMUs being attacked $P_a$ with (a) fault on Line 21 – 22 and (b) fault on Line 14 – 15.](image)

### 3.3.5 Discussion

We propose a novel measurement-based multi-flock technique for real-time generator coherency identification that works rapidly and accurately in the presence of serious system fault or attack. We compare the performance of our approach with existing techniques and evaluate its effectiveness in three situations: an ideal environment, a noisy environment, and an environment under cyber attack. The simulation results demonstrate how our approach achieves high identification accuracy even with very short observation windows and in the presence of environmental noise and cyber attack. We believe these advantages demonstrate the potential our
technique as an effective tool for rapid and robust generator coherency identification in emerging smart grid systems, especially for applications requiring maintaining transient stability of wide-area power systems.

3.4 Witness-Based Security Protocol for Information Corruption Mitigation

This section represents a witness-based security protocol which builds on the two-tier hierarchical cyber-physical framework introduced in Section 3.2 and considers a cyber-physical viewpoint to the problem of data corruption in smart grid systems. This protocol takes the perspective that one may leverage natural physical couplings amongst power system components as telltale signs to identify information corruption.

3.4.1 Literature Review

Recent work focused on false data injection attacks has demonstrated how an opponent can bias power system measurements and overcome residual-based bad data detection approaches [76]. Subsequent research has focused on identifying such attacks [80, 93, 98] and has largely taken an information perspective. More recently, the smart grid security community has been considering cyber-physical perspectives [147].

3.4.2 Problem Setting

We consider the two-tier hierarchical cyber-physical multi-agent framework introduced in Section 3.5 to model the smart grid stability problem in a smart grid system, in which the agents within the same cluster exhibit high physical coherence. Inter-cluster PMU communications involves data exchange amongst lead agent PMUs through a multi-hop network consisting of source/sink nodes which are the lead agents’ PDCs. Intra-cluster PMU communications occurs through a local area network (LAN) whereby the PDC acts as an aggregator. The PDC also aligns the PMU data prior to sending information to a local controller.

The two-tier hierarchical smart grid protection framework exploits generator coherence to activate local cyber control only at lead generators of clusters. Moreover, it is shown that only lead agent PMU information is needed to ensure the system stabilization in the face of a disturbance (even if the fault is cleared after the critical clearing time (CCT)). The objective of the active controllers is to achieve lead agent frequency synchronization in the face of cyber-physical disturbance. The secondary generators achieve synchronization via strong physical
couplings with a stabilized lead generator. The resulting adaptive cyber-physical system exhibits a hierarchical structure whereby inter-cluster interactions are cyber-physical (tier-1) and intra-cluster synergies are physical (tier-2). A natural question arises as to the effects of lead agent PMU data corruption on the system stabilization capabilities of the system.

In this section, we build upon this natural system hierarchy to develop an approach to defend against information corruption. Essentially, the PMU data from the lead agents is validated using the PMU data from the secondary agents. Our approach can identify cyber attack assuming there is an upper limit on the number of simultaneously corrupted PMU readings. During verification, the PDC works as an aggregator in the intra-cluster LAN to detect corrupted data from the lead agent’s PMU and, if needed, estimate the true value via communicating with secondary agent’s PMUs.

### 3.4.3 Witness-Based Verification and Estimation Protocol

The PMUs of the lead agents in our two-tier framework provide critical measurements for maintaining smart grid stability. Therefore, detection of possible lead PMU data corruption and subsequent real-time estimation are necessary for smart grid stability maintenance. In order to address this problem, we propose a cyber-physical verification and estimation protocol developed under the following threat model, as illustrated in Fig. 3.12.

![Figure 3.12: Communication between PDC and agents locally within each cluster.](image)

**Threat Model:** Let $H_k$ be the number of agents in the $k$th cluster of our proposed two-tier hierarchical framework. An attack can corrupt up to $\left\lfloor \frac{1}{2} H_k \right\rfloor$ PMU measurements where $\lfloor \cdot \rfloor$ denotes the floor function. Corruption constitutes biasing PMU readings or equivalently replacing true values with fabricated quantities over a verification period.
Let the lead agent PMU reading be $\theta^c$. Let the secondary agents be represented with indices from the set $i \in I$ and their readings be denoted $\theta_i$. Let $\Delta \theta_i$ be the phase angle difference between $\theta_i$ and $\theta^c$ at static state (i.e., pre-fault). We assign $H_k = |I| + 1$.

1. Initialize $Count = 0$ and set the threshold $\tau_p$.

2. For each $i \in I$
   \[ \xi_i = \theta_i - \Delta \theta_i - \theta^c, \]
   If $\xi_i \leq \tau_p$
   \[ Count = Count + 1, \]
   End

3. If $Count < \lfloor \frac{1}{2} H_i \rfloor + 1$
   The PDC reports the lead agent’s PMU as being attacked,
   Else
   The PDC reports the lead agent’s PMU as valid,
   End

The false data injection attack can be conducted by manipulating the PMU readings physically or compromising the LAN between the PMUs and the PDC [148]. As described in Eq. (3.5), the states of the secondary agents can be considered noisy estimates of the states of their lead. Based on this fact, our verification protocol treats the secondary agents as “witnesses” with their PMU data representing redundant information to measure the trustworthiness of the PMU readings of the lead agents.

In the intra-cluster LAN, the PDC must therefore probe the PMU data from secondary agents (at a lower data rate than for lead PMUs called the verification rate). Using the received data, the PDC measures the trustworthiness of a lead agent’s PMU using the verification scheme described in Table 3.7. Since our proposed flocking-based control protocol is robust to the biases on the measurement of the lead agents’ frequency [149], we address detection and mitigation of the compromised reading on the lead agents’ phase angle.

At the end of each verification procedure, if the PDC concludes that the lead agent’s PMU is valid, it stores the $\ell$ most recent bias samples $\{\xi_i | i \in I\}$ for possible future estimation use. Otherwise, it estimates the true value using the proposed cyber-physical estimation scheme of Table 3.8.

The PDC then uses the estimated value for calculation of $P_u$ and increases the verification probe rate to that of the sampling rate of the lead agent PMUs until it concludes the reading of the lead agent’s PMU is valid for two consecutive verification periods or an operator deems the lead PMU reading authentic. Convergence of the algorithm of Eq. (3.8) is guaranteed
Table 3.8: Proposed Cyber-Physical Estimation Scheme

Let the secondary agents be represented with indices from the set \( i \in \mathcal{I} \). Let \( \xi_i \in \mathbb{R}^\ell \) be a vector containing the \( \ell \) most recent sample values of \( \xi_i \) in chronological order. Let \( a(n) \) be an \( \ell \)-point Hamming window.

1. For each \( i \in \mathcal{I} \)
   - Secondary agent estimates lead agent phase angle using Eq. (3.5).
   - Secondary agent reports the estimation result \( \hat{\theta}_i^c \) to the PDC.

2. The PDC evaluates estimation accuracy for \( i \in \mathcal{I} \) by computing:
   
   \[
   \hat{\sigma}_i = \sqrt{\frac{\sum_{n=1}^{\ell} a(n-1) \xi_i(n)^2}{\sum_{n=1}^{\ell} a(n-1)}}. \tag{3.34}
   \]

3. The PDC forms \( \hat{\theta}_l \) consisting of elements \( \hat{\theta}_i^c \), \( i \in \mathcal{I} \) ordered to reflect monotonically increasing values in \( \hat{\sigma}_i \).

4. The PDC estimates \( \hat{\theta}^c \) from a median-like value from the elements of \( \hat{\theta}_l \) to avoid extreme biases:
   
   \[
   \hat{\theta}^c = \begin{cases} 
   \frac{1}{2} \hat{\theta}_l \left( \frac{1}{2} H_k \right), & \text{if } H_k \text{ is even;} \\
   \frac{1}{2} \left[ \hat{\theta}_l \left( \frac{1}{2} (H_k - 1) \right) + \hat{\theta}_l \left( \frac{1}{2} (H_k - 1) + 1 \right) \right], & \text{otherwise}
   \end{cases}
   \]
analytically [150], but witness-based protocol performance is studied empirically.

Therefore, our proposed cyber-physical verification and estimation schemes both aim to leverage the hierarchy of the physical interaction amongst agents to achieve low computational complexity, which facilitates scalability and real-time implementation. Our verification scheme adopts a dynamically adjustable verification rate to optimally reduce bandwidth usage. When the PDC reports an attack on the lead agent’s PMU, our estimation scheme employs a short Hamming window to estimate the true value of the attacked PMU’s readings, which includes the historical information to improve the estimation accuracy and also assigns a higher priority to the current data. Moreover, our estimation achieves high robustness to potential attacks on the secondary agents’ PMUs by choosing the median-like value rather than a weighted average for the final estimation result.

3.4.4 Discussion

In this section, we demonstrate through extension of our flocking-based cyber-physical system framework, the effectiveness of a witness-based approach to identify and mitigate information corruption in a smart grid distributed control problem for smart grid stability. Our proposed hierarchical cyber-physical protection framework addresses both cyber (e.g., information corruption) and physical (e.g., faults and their latent clearing) disruptions. Simulations on the 39-bus New England test system demonstrate the potential of our protocol and verification scheme.

We assert that the strength of our scheme is in the effective use of state-dependent hierarchy. Information is exploited to provide a novel distributed control paradigm for smart grid stability in the presence of physical disturbances while physical coherence is leveraged so that information can be selectively used for robustness to cyber attack.

3.5 Simulations and Performance Assessment

We demonstrate the performance of our flocking-based two-tier hierarchical control framework with dynamics in Eqs. (3.8) and (3.9) collectively also described by Eq. (3.2) in achieving smart grid stability for two case studies on the New England 39 Bus system as shown in Fig. 3.13 and detailed in [1] consisting of $C = 10$ generators. MATLAB/Simulink is employed for simulations. As illustrated in Section 2.5, if our proposed control protocol is able to successfully maintain smart grid stability without taking into account governor control systems with appropriate settings, we can always conclude that our control protocol is efficient in maintaining smart grid stability by considering governor control systems. This is because of the governor
control system’s function on improving the phase angle stability and frequency stability of the power system. Therefore, in this section, we only evaluate the performance of our proposed hierarchical control framework without taking into account governor control systems. In each case, we illustrate the efficiency of our proposed two-tier hierarchical control framework in selectively leveraging physical couplings to apply cyber data and control selectively. In all (non-hierarchical and hierarchical) cases the cyber control parameters of Eq. (3.16) are set to $c_1 = 5$, $c_2 = 3$, and $c_3 = \frac{1}{10}$, the parameters for agent coherency identification is shown in Table 3.5, and the PMU sampling rate is 50 Hz. The power transmission limit for the fast-acting grid is set to $\mu = \frac{P_u,i}{P_r,i} \leq 1$ where $P_r,i$ is the rated power.

Figure 3.13: New England 39-bus power system.

We compare our results to situations when no control is computed nor applied (corresponding to minimum information use and control) and when non-hierarchical control is applied (corresponding to maximum information use and control). An efficient hierarchical framework would have comparable stabilizing performance to the latter case without the associated overhead. In each case, we also evaluate the performance of our hierarchical framework when experiencing cyber communication delay and practical constraints of fast-acting EES.

3.5.1 Ideal Environment

3.5.1.1 Case I

The system disturbance consists of a 3-phase short circuit in the middle of Line 14 – 15 of Fig. 3.13 which occurs at time $t = 0$ s. The Line 14 – 15 is removed at $t = 0.1$ s. Fig. 3.14 shows the normalized rotor frequencies and phase angles over a period of 10 s when no control is applied corresponding to Eq. (3.3) for $\alpha_i = 0$ for all $i$. Instability is clearly evident in all plots.
Our two-tier hierarchical cyber-physical control framework is implemented in the following three steps. 1) the proposed timely dynamic agent coherency identification scheme is implemented immediately after Line 14 – 15 is removed at time $t = 0.1$ s. The corresponding flockmate trajectories introduced by the flocking analogy used in our agent coherency identification scheme is presented in Fig. 3.17(a) for a very brief observation period of $t = 0.05$ s;
as described in Eq. (3.25), each flockmate carries the information describing the associated agent’s status. The neighboring flockmates interact with each other based on the informational similarity which is defined in Eq. (3.27) and their dynamics are modeled in Eq. (4.17). From Fig. 3.17(a), we observe that the agent coherency involving the following groups: \{Agent_1\}, \{Agent_2, Agent_3\}, and \{Agent_4, \ldots, Agent_{10}\}. 2) Based on the achieved result on agent coherency, we determine that our two-tier hierarchical framework consists of the clusters \{Agent_1\}, \{Agent_2, Agent_3\}, and \{Agent_4, \ldots, Agent_{10}\}, and the lead agents for these three clusters are Agent 1, Agent 3 and Agent 4, which have larger inertia compared with other agents belonging to the same cluster. 3) After determining the hierarchical framework, at time $t = 0.15$ s, our proposed two-tier hierarchical cyber-physical control framework is activated which controls the fast-acting EES associated with each lead agent to absorb/inject power to the generator buses of the associated agents. Based on our proposed control framework, the power absorption/injection is calculated based on Eq. (3.16) and is plotted in Fig. 3.17(b). As shown in Fig. 3.17(b), the EESs of the Lead Agents 1, 3, 4 are activated to absorb power from the system at time $t = 0.15$ s and then adjust their power output at each time step $\Delta t = 20$ ms to track the command given by the associated local controllers. After time $t = 0.25$ s the power output of each EES sinusoidally decays to zero. In contrast to the EES power outputs for non-hierarchy, the sinusoidal oscillations are higher in frequency. This is because the hierarchical case represents an “under-actuated” version of the nonhierarchical such that the control applied to select generators must stabilize all of them. This requires that the associated control signals to be more “reactionary” and faster-moving.

Figure 3.18 presents the generator frequencies and phase angles by using our proposed two-tier hierarchical cyber-physical control framework. In contrast to Fig. 3.14 in which there
Figure 3.17: (a) The trajectories of the flockmates for Case Study I and (b) power transfer $P_u$ by fast acting energy storage at generator buses in the presence of hierarchical control for Case Study I.

is no control, smart grid stabilization is evident. In contrast to the non-hierarchical case shown in Fig. 3.15, there is more high frequency oscillatory behavior due to the nature of the activated EES power outputs. From Fig. 3.18, we deduce that although the information acquisition and control is selectively applied to lead agents only, the high physical coherency between the secondary agents and their associated agents ensures maintaining the smart grid stability of all the agents.

Figure 3.18: (a) Normalized rotor frequencies and (b) phase angles with hierarchical control.

3.5.1.2 Case II

The system disturbance consists of a 3-phase short circuit occurs at time $t = 0$ s in the middle of Line 17 – 27 of Fig. 3.13. The Line 17 – 27 is removed at $t = 0.1$ s. Figure 3.19 shows the
normalized rotor frequencies and phase angles over a period of 10 s when no control is applied. Based on Fig. 3.19, we assess smart grid stability of the system by calculating the power angle-based stability margin \( \xi \) [116], and achieve \( \xi_1 = 57.1 \) which implies that the system smart grid security is low and very sensitive to perturbation. Parameter \( \xi = \frac{360 - \delta_{\text{max}}}{360 + \delta_{\text{max}}} \times 100 \) where \( \delta_{\text{max}} \) is the maximum angle separation of any two generators at the same time in the post-fault response, and \(-100 < \xi < 100\).

![Figure 3.19: (a) Normalized rotor frequencies and (b) phase angles without cyber control.](image)

To relax the angle-based stability margin to improve the system’s smart grid security after fault, we implement our hierarchical control framework, in which the outputs of fast-acting energy storage are controlled to compensate for demand power’s fluctuations caused by the 3-phase short circuit fault. Our timely dynamic agent coherency identification scheme is implemented immediately after Line 17 – 27 is removed at time \( t = 0.1 \) s. The corresponding flockmate trajectories introduced by the flocking analogy used in our agent coherency identification scheme is presented in Fig. 3.20 for a very brief observation period of \( t = 0.05 \) s. From Fig. 3.20, we determine that our two-tier hierarchical framework consists of the clusters \( \{ \text{Agent}_1, \text{Agent}_{10} \} \), \( \{ \text{Agent}_2, \ldots, \text{Agent}_8 \} \), and \( \{ \text{Agent}_9 \} \), and the lead agents for these three clusters are \( \text{Agent}_1 \), \( \text{Agent}_4 \) and \( \text{Agent}_9 \). After determining the hierarchical framework, our proposed two-tier hierarchical cyber-physical control framework is implemented during time \( t = 0.15 \) s to 3 s, which is critical maintenance duration.

Figure 3.21 evaluate the performance of normalized rotor frequencies and phase angles by using our proposed hierarchical control framework and Figure. 3.22 shows the power transfer from the fast-acting energy storage to each generator bus. We achieve the angle-based stability margin \( \xi_2 = 70.7 \), which validates our framework is efficient in improving the smart grid security of the power system after severe fault.
Figure 3.20: The trajectories of the flockmates for Case Study II.

Figure 3.21: (a) Normalized rotor frequencies and (b) phase angles with hierarchical framework.

Figure 3.22: Power transfer $P_u$. 
3.5.2 Environment With Practical Constraints of Energy Storage

We evaluate the performance of our hierarchical framework by considering the practical constraints of fast-acting energy storage on power output $P_u$. We assume the energy storage associated with each Agent $i$ has two constraints: 1) the power output $|P_{u,i}| \leq \rho_1$ p.u., and 2) the rate of the power change $|\Delta P_{u,i}| \leq \rho_2$ p.u./$\Delta t$, where $\Delta t = 20$ ms denotes the time step for calculating the control signal for $P_{u,i}$. In the simulation, we consider the same two cases in previous section. Figure 3.23 evaluates, given different values of $\rho_1$, the minimum value of $\rho_2$ required for maintaining smart grid stability by using hierarchical and non-hierarchical frameworks in Case I. Figure 3.23 also evaluates the minimum value of $\rho_2$ required for improving $\xi$ equivalent to ensuring $\xi > 57.1$ versus different values of $\rho_1$ by using hierarchical and non-hierarchical frameworks in Case II. From Fig. 3.23, it is clear that in Case I, compared to the non-hierarchical framework, the hierarchical framework requires higher but comparable physical requirement for energy storage when $\rho_1 \leq 8$. Figure 3.23 also indicates that in Case II, the hierarchical and non-hierarchical framework desire the same physical requirement for energy storage.

![Figure 3.23: Performance evaluation of Cases I and II by considering physical constraints of fast-acting energy storage.](image-url)

In order to analyze the performance of our proposed control framework under the two constraints in more detail, Fig. 3.24 evaluates the power angle-based margin $\xi$ achieved by implementing our control framework when $\rho_1 \in [1, 5]$ and $\rho_2 \in [0.1, 0.5]$. From Fig. 3.24(a), it is clear that in Case I the proposed hierarchical framework is able to maintain smart grid stability when $\rho_1 \leq 4.5$ and $\rho_2 \geq 0.2$, or $\rho_1 = 5$ and $\rho_2 \geq 0.2$. From Fig. 3.24(b), it is clear that in Case II the proposed hierarchical framework is able to improve the stability margin when $\rho_1 \leq 5$ and $\rho_2 \geq 0.1$. Based on the above observation, we can get that the constraints of the power output and the rate of the power output jointly impact on the performance of
the proposed control framework. Furthermore, in both cases, better stability margin can be achieved by implementing the non-hierarchical control framework, but the performance of the hierarchical control framework is comparable with that of the non-hierarchical framework. Therefore, the conclusions obtained from Fig. 3.24 are consistent with the conclusion got from Fig. 3.23. We believe it is reasonable that under the practical physical constraints the non-hierarchical control framework achieves slightly better results than the hierarchical framework. This is because that in the non-hierarchical framework, more fast-acting ESSs are activated which mitigates the impact of the constraints associated with each ESS.

![Graph showing stability margin achieved under practical constraints](image)

Figure 3.24: The stability margin achieved under the practical constraints in (a) Case Study I and (b) Case Study II.

Figure 3.25 shows the transfer power $P_u$ between the ESS and the power system by implementing our proposed hierarchical control framework under the constraints $\rho_1 = 2$ and $\rho = 0.3$ in Case I, and Fig. 3.26 shows the generators’ normalized rotor frequency and phase angle in this case study. From the simulation results, it is clear that our proposed framework is able to efficiently to maintain smart grid stability under the practical physical constraints of the fast-acting ESSs.

### 3.5.3 Environment With Communication Delay

We evaluate the performance of our hierarchical framework by considering unexpected communication delay of the PMU data associated with the “lead” agents. As stated in [151–153], in smart grid, the communication delay is a significant problem in the application of smart grid and it is usually caused by high network congestion or cyber attack such as Denial-of-Service (DoS) attack. For example, as stated in the news published at eurativ.com on 10 Dec. 2012, a German renewable power grid was hit by a serious communication delay caused by DoS.
Figure 3.25: Power transfer $P_u$ by fast acting energy storage at generator buses.

Figure 3.26: (a) Normalized rotor frequencies and (b) phase angles versus time.
attack [154]. Besides the already happened incidents, various researches are also being developed to study the impact of the potential communication delay caused by network congestion or DoS attack [155–157].

We consider both of the fixed and random communication delay in the cases studied in the previous section. In each case, we consider the situation that there is unexpected communication delay during time $t = 0.2$ s to $t = 3$ s, which is within the critical duration for smart grid stability maintenance. Considering the communication delay, the phasor data concentrator (PDC) of each cluster employs the following rules: 1) The PMU data received by PDC of each cluster are buffered to guarantee synchronization of the PMU data used in local controller. 2) Until updated again, the control signal $P_u$ is kept the same as the last updated value. 3) If all the PMU data with time stamp $t = k$ are received while the data with time stamp $t = k - 1$ are still buffered, the previous data are dropped and $P_u$ is calculated based on the PMU data with time stamp $t = k$.

### 3.5.3.1 Fault on Line

We first consider the situation of fixed communication delay. The performance of normalized frequencies and phase angles are shown in Fig. 3.27. From Fig. 3.27, we observe that our hierarchical framework still maintain the smart grid stability of the system. This demonstrates resilience of our hierarchical framework to communication delay. Compared with the simulation results without considering the communication delay, which is shown in Fig. 3.18, the generator frequencies and phase angles both vibrate in much higher frequency before time $t = 3$ s. This is reasonable. Because of the communication delay, the commands used to control the ESSs’ outputs are calculated based on the historical system information, which reduces the accuracy and timeliness of the commands. Therefore, the commands have to be adjusted with much higher frequency in order to ensure the smart grid stability maintenance. The higher-frequency adjustment of the ESSs’ outputs cause the higher-frequency vibration of the generators’ frequencies and phase angles.

We also consider the situation with random communication delay. The random communication delay $\tau$ is modeled based on the packet service time statistics in $M/M/1$ queueing system and generated from a Poisson distribution as follows: [158]:

$$p(\tau) = \frac{1}{\kappa} e^{-\frac{\tau}{\kappa}},$$

where $\kappa$ denotes the average service time, which is equivalent to average communication delay in our framework.

Setting the average communication delay as 60 ms, the performance of normalized fre-
Figure 3.27: (a) Normalized rotor frequencies and (b) phase angles with hierarchical control when considering fixed communication delay.

Figures and phase angles are shown in Fig. 3.28. From Fig. 3.28, we can get that compared with the situation with fixed communication delay, the random communication delay having the same average value causes vibration with larger amplitude of the generator frequencies and phase angles. The figures also validates the resilience of our hierarchical framework to random communication delay.

Figure 3.28: (a) Normalized rotor frequencies and (b) phase angles with hierarchical control when considering random communication delay.

Table 3.9 illustrates the comparison between the performances in smart grids stability maintenance by using non-hierarchical cyber-physical control framework and using two-tier hierarchical cyber-physical control framework. From Table 3.9, it is clear that in this case study, these two frameworks have the same resilience to fixed communication delay for maintaining smart grid stability, and the hierarchical framework has higher resilience to random communication delay for maintaining the smart grid stability. This is reasonable. The non-hierarchical control framework requires more data acquisition and the hierarchical control framework. Therefore,
the communication delay has bigger impact on the non-hierarchical control framework than on the hierarchical one. When the communication delay is fixed, the communication delay impacts equally on each activated ESS’s output. Therefore, for maintaining smart grid stability, the difference of the overall impacts of the fixed communication delay by using these two control framework is much less than the difference of the overall impacts of the random communication delay by using these two control framework. In this case study, the impact of fixed communication delay on these two control framework for smart grid stability maintenance are not distinguishable, while the impact of random communication delay on the non-hierarchical framework is obviously larger than on the hierarchical framework. Therefore, in general, the hierarchical framework shows its advantage in resilience to communication delay by highly reducing the cyber information acquisition.

Table 3.9: Comparison Between Performances of Non-Hierarchical and Hierarchical Frameworks

<table>
<thead>
<tr>
<th>Framework</th>
<th>With fixed delay</th>
<th>With random delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Hierarchical</td>
<td>Smart grid stability is maintained when $\tau \leq 130$ ms</td>
<td>Success rate is above 95 % when $\kappa \leq 60$ ms</td>
</tr>
<tr>
<td>Hierarchical</td>
<td>Smart grid stability is maintained when $\tau \leq 130$ ms</td>
<td>Success rate is above 95 % when $\kappa \leq 110$ ms</td>
</tr>
</tbody>
</table>

### 3.5.3.2 Fault on Line 17 – 27

The performances of hierarchical and non-hierarchical framework in improving the power angle-based stability margin $\xi$ are evaluated in Fig. 3.29. Figure 3.29(a) considers the situation with fixed communication delay and plots the stability margin $\xi$ versus the value of communication delay. Figure 3.29(b) considers the situation with random communication delay and plots the stability margin $\xi$ versus the value of average communication delay. From Fig. 3.29(a), it is clear that when the fixed communication delay $\tau \leq 90$ ms, employing the non-hierarchical framework achieves slightly better stability margin than employing the hierarchical framework. However, when $\tau > 90$ ms, the performance of the non-hierarchical framework becomes dramatically worse compared with the performance of hierarchical framework.

As stated in Section 3.5.1.2, the stability margin of the system is $\xi = 57.1$ when no control is applied. From Fig. 3.29(a), we observe that to achieve an improvement in stability margin, the fixed communication delay should be $\tau \leq 110$ ms for nonhierarchical control and $\tau \leq 140$ ms using the hierarchical framework. From Fig. 3.29(b), we also observe that for random communication delay $\kappa \geq 20$ ms, the performance of the nonhierarchical framework
becomes dramatically worse compared to the performance for the hierarchical framework. To improve the stability margin over the no control case, the average communication delay should be $\kappa \leq 40$ ms and $\tau \leq 100$ ms for the nonhierarchical and hierarchical cases, respectively thus demonstrating the greater negative impact of random delay on the performance of both hierarchical and nonhierarchical frameworks.

Figure 3.29: Stability Margin $\xi$ in the situation considering (a) fixed communication delay and (b) random communication delay.

3.5.4 Environment With PMU Data Corruption

We evaluate the performance of our witness-based security protocol in Case I by considering unexpected information corruption of the PMU data associated with the “lead” agents. In the simulation, we consider the practical constraints with the energy storage $\rho_1 = 2$ and $\rho_2 = 0.3$. Furthermore, the PMU sampling rate is assigned as 50 Hz, the verification probe rate is initially set to 5 Hz (no-attack condition) and then raised to 50 Hz after lead generator attack detection, and $\ell = 50$. The threshold in Table 3.7, $\tau_p = 35^\circ$.

3.5.4.1 Random Attack

Figures 3.30 and 3.31 show the normalized frequencies, rotor phase angles, and $P_u$ in the presence of “random” bias attack when no witness-based cyber protection is applied. The attack specifically consists of PMU corruption of Agents 4, 6 and 7 at $t = 0.2$ s for duration 7.5 s, 6.5 s, and 6 s with biases $-160^\circ$, $120^\circ$, and $240^\circ$, respectively. From Figs. 3.30 and 3.31, it is clear that the corrupted readings mislead the PDC of the third cluster, result in a miscomputation of $P_{u,3}$ and subsequent instability results.

Figures 3.32 and 3.33 show the normalized rotor frequencies, phase angles and $P_u$ when our cyber-physical control and witness-based protection protocol is applied. We observe the
Figure 3.30: (a) The normalized frequencies and (b) the rotor phase angles versus time without proposed cyber-physical security protocol in presence of random attack.

Figure 3.31: $P_u$ versus time without proposed cyber-physical security protocol in presence of random attack.
stabilizing performance of our proposed protocol in verifying the validity of the readings of the lead agents’ PMUs and estimating their true values. Smart grid stability is still maintained in the presence of the random attack.

![Figure 3.32](image)

(a) The normalized frequencies and (b) the rotor phase angles versus time with proposed cyber-physical security protocol in presence of random attack.

![Figure 3.33](image)

Figure 3.33: $P_u$ versus time with proposed cyber-physical security protocol in presence of random attack.

### 3.5.4.2 Collusion Attack

Figures 3.34 and 3.35 show the situation in which the compromised PMUs of Agent 4, 6 and 7 collude and report the same biased readings (bias = $-160^\circ$) starting at $t = 0.2$ s for duration 7.5 s, 6.5 s, and 6 s, respectively.

Figures 3.36 and 3.37 demonstrate that our proposed security protocol is still robust to this type of collusion since the number of corrupted PMU measurements $\ell = 3$ is less than or equal to $\left\lfloor \frac{1}{2} H_k \right\rfloor$ where $H_k = 7$, which obeys our threat model of Section 3.4.

These simulation results illustrate that our proposed cyber-physical verification and estimation schemes can efficiently identify and correct the corrupted lead agents’ PMUs’ readings.
Figure 3.34: (a) The normalized frequencies and (b) the rotor phase angles versus time without proposed cyber-physical security protocol in presence of random attack.

Figure 3.35: $P_u$ versus time without proposed cyber-physical security protocol in presence of random attack.

Figure 3.36: (a) The normalized frequencies and (b) the rotor phase angles versus time with proposed cyber-physical security protocol in presence of smart attack.
to aid in successful maintenance of the smart grid stability. The simulation results also help demonstrate robustness against attacks on the secondary agents’ PMUs as long as our threat model of Section 3.4.3 is satisfied.

### 3.6 Conclusions

It is well known that information will play an important role in enhancing emerging smart grid system operation. Questions therefore naturally arise as to when the increased data-dependence may be considered excessive. Two practical considerations emerge: 1) communications and computational overhead, in which redundant and irrelevant information acquisition and use results in heavy computational burden with limited performance return, and 2) increasing risks of power system disruption due to information delay from communication congestion or cyber attack. One strategy to improve smart grid resilience is to determine the appropriate degree of dependence on cyber information to balance performance with overhead and risk. In this chapter, we present a hierarchical cyber-physical multi-agent model of smart grid system operation based on flocking theory in the context of the transient stability problem. Through this model, we study strategies that harness a selective degree of cyber technology by leveraging physical couplings. Our formulation enables the identification of large-scale distributed control strategies for robust and resilient power grid operation. We demonstrate the potential performance improvements of our findings on the New England 39-bus power system for case studies involving a variety of system faults and communication delays.

In order to exploit the physical coherence efficiently and timely, in Section 3.5, we propose a novel multi-flock-based technique to identify generator coherence rapidly within a short observation window. Our measurement-based approach transforms generator data from the
observation space to an information space whereby the generator frequencies and phases characterize the movement and dynamics of flockmates within multiple flocks. Analysis of the flockmates’ trajectories enables the discrimination of multiple flocks, corresponding to coherent generator clusters. Besides being used in the proposed hierarchical cyber-physical control framework, the proposed generator coherency identification method is believed to establish itself as an important tool to aid in the other applications of resistance of cascading failures within wide-area power systems.

Furthermore, based on the proposed hierarchical cyber-physical control framework, we also consider a cyber-physical perspective to the problem of identifying and mitigating information corruption in smart grid systems. In Section 3.4, we study the problem of transient stability with distributed control using real-time data from geographically distributed phasor measurement units via a flocking-based modeling paradigm. We demonstrate how cyber corruption can be identified through the effective use of telltale physical couplings within the power system. We develop a novel witness-based cyber-physical protocol whereby physical coherence is leveraged to probe and identify phasor measurement unit data corruption and estimate the true information values for attack mitigation.
Chapter 4

GOAliE: A Resilient Multicast Routing Approach in Smart Grids

4.1 Introduction

It is well known that the smart grid involves the integration of advanced measurement, communications and control with the power delivery system. Phasor measurement units (PMUs) provide precise time-stamped voltage, current and frequency information at acquisition rates ranging from $10^{-250}$ Hz at select locations of the grid [159]. The effectiveness of such high fidelity data for grid monitoring and control is subject to communication timing guarantees [160]. As a result, the North American Synchrophasor Initiative (NASPI), a joint effort between the U.S. Department of Energy (DOE) and the North American Electric Reliability Corporation (NERC), recently developed a reference communication infrastructure called NASPI network (NASPInet) to support PMU data delivery and specify recommended smart grid data delivery requirements including those related to latency and reliability [161, 162].

Since its proposal several communication networking research thrusts have focused on NASPInet requirements. Recently, the authors of [163] proposed a centralized framework that optimizes the placement of trust nodes enabled with security services within the communication network and finds the least cost routing through such nodes. The approach has potential to achieve global efficiency and security, but its centralized structure limits scalability to large networks. In [164], a hybrid decentralized network architecture is proposed where routing decisions are based on dynamic network formation games to improve reliability. However, the efficiency of this unicast architecture is reduced for heavy traffic. In [5], the authors employ flocking principles to model smart grid information flow for routing over multi-hop mesh networks that accounts for latency and denial-of-service (DoS). Although the flocking paradigm
has potential, the unicast nature of routing is performance-limiting for high traffic.

Recent studies have demonstrated the potential of multicast publish-subscribe network architectures to achieve the NASPInet requirements of low latency and high reliability [160, 165]. GridStat [166, 167] is a quality of service (QoS)-managed network architecture based on a publish-subscribe paradigm. Here, the PMU data is delivered through a network of middleware-level status routers. Routing paths are determined by a hierarchical QoS management plane to achieve low latency and high reliability. Since routing computations are conducted offline, support currently does not exist to react to short-term changes in traffic. To address this issue, in [159] a cooperative congestion control (CCC) framework for real-time route determination in the GridStat is proposed. However, the authors only describe the general functions of CCC rather than provide implementation details. In [168], a detailed multicast routing implementation is proposed for smart grid voltage control. Routing is formulated as an optimization problem assuming a simplified model of the physical system and heuristic solution approaches are applied. Questions arise as to its applicability to complex real-world smart grid topologies.

In this chapter, we propose a quality-of-experience (QoE)-managed network architecture based on a publish-subscribe paradigm. In our framework, multicast routing protocol is implemented through a multi-hop mesh networking framework commonly investigated with respect to smart grid applications. We focus on the development of a mathematical model to describe information flow that is compatible with existing models of power flows and does not require a simplification of physical system dynamics. To address the interaction between the physical system and routing protocol, we exploit the coupling between network packets carrying related measurement data to exchange valuable route experience information. Furthermore, our QoE-based multicast routing philosophy aims to be efficient and adaptive to unexpected traffic congestion and DoS.

### 4.2 Problem Setting

We consider a general two-tier hierarchical multi-agent-based framework for smart grid presented in Chapter 3 in which an agent consists of both cyber and physical elements: (1) a dynamic (physical) generator node, (2) a (cyber) PMU that acquires data such as phase angle and frequency from the generator node, and (3) a local (cyber) controller that, if activated, obtains information from its PMU and others to compute a control signal that is applied to the generator node of the same agent.
4.2.1 Hierarchical Structure

The hierarchical structure applies to common distributed smart grid contexts. Here, agents with generators exhibiting high physical coherence are said to form a cluster. Each cluster also consists of a phasor data concentrator (PDC) as well as dedicated power or storage source external to each agent often used for control. To reduce overhead, only one “lead” agent within the cluster is selected such that only it participates in cyber communication and control during operation, and its strong physical coupling to other agents’ generators is exploited to regulate the overall cluster [169]. In this way inter-cluster interactions are cyber-physical (tier-1) and intra-cluster synergies are physical (tier-2).

![Hierarchical cyber-physical framework](image)

Figure 4.1: Hierarchical cyber-physical framework for the New England 39-bus Power System.

We illustrate our hierarchical communication framework for the well-known New England 39-bus system in Fig. 4.1. Here, we assume there are four clusters and the lead agent of each cluster is denoted with a shaded (green) generator. Effective PMU information (cyber) and power (physical) flows are presented as dashed and solid arrows, respectively. To further delineate the tiered nature of communications, red, blue and magenta dashed arrows represent tiered communications from lowest to highest level.

The PMU information flows between lead agents are realized by the wide area multi-hop mesh network of Fig. 4.2 successfully studied by a variety of authors for smart grid [159, 166, 170, 171]. The network consists of lead agents representing sources and sinks, relay nodes and
finite capacity communication links. At a given time index, the lead agents generate the packets
and release them into the network for distributed propagation to the destination. The packets
complete the propagation successful through the interaction with the network infrastructure
and other traveling packets. To enable real-time guarantees in the face of network attack and
congestion, we study a dynamic, distributed multicast routing protocol based on robust flocking
principles.

4.2.2 Flocking for Routing

Flocking is a behavior exhibited by groups of birds participating in a shared objective that is
difficult to achieve individually, but is possible through cooperation, consensus and informed-
adaptation. Members of a flock are referred to as flockmates or agents. Flocking behavior has
been described by a set of heuristic agent-interaction rules [122, 172]:

1. **flock centering**: agents attempt to stay close to nearby flockmates,

2. **velocity matching**: agents attempt to match velocity with nearby flockmates,

3. **goal seeking**: each agent has a desired velocity towards a specified position in global space,

4. **obstacle evasion**: agents evade obstacles often steering away from their goals

5. **collision avoidance**: agents avoid collisions with nearby flockmates,
6. **behavioral transitions**: past experience of the collective influences future behavior unbeknownst to individual flockmates.

We have formerly investigated the first three agent-interaction rules to reformulate the problem of smart grid stability in smart grid systems to one of flocking-based distributed multi-agent control as presented in Chapters 2 and 3. Analogies of *flock centering* to generator phase angle cohesiveness, and *velocity matching* and *goal seeking* to exponential generator frequency synchronization were established requiring wide area monitoring and communications be present.

In this chapter, we apply flocking principles to develop a routing philosophy that aims to defend against DoS attack and balance end-to-end latency, bandwidth consumption and fairness for the wide area communications. We contend that for such applications, subsets of communications streams must be synchronized to be useful for critical real-time monitoring and control. Moreover, communications must be cooperative to make collective timing guarantees hence making the application of flocking models appealing also in this context.

In the next section, we demonstrate that successful principles for flocking provide valuable insight for the development of a resilient routing protocol for smart grid. We propose a novel approach for multi-objective dynamic multicast communications that is reactive to changing network environment to facilitate the need for resilience in smart grid. We model multicast packet replication and route splitting as flock separation whereby a group of flockmates (collectively representing a multicast packet) experience forces of repulsion and attraction to one another based on routing objectives and network conditions. Finally, to promote self-healing networking, our routing paradigm employs experiential information from “predecessor” flockmates for adaptive congestion and DoS control.

### 4.3 Goal-Seeking Obstacle and Collision Evasion (GOAliE) for Multi-Cast Smart Grid Routing

Within our framework, we denote a packet being processed and transmitted in the network as *active*. Each such packet is generated at a given time index by its source and released for distributed multicast propagation to its destination(s) through interaction with network infrastructure and other flockmates. Packets generated from the same source within the same communications session are said to comprise a 3-D *flock* with each member being a *flockmate*.

Fig. 4.3 illustrates a PMU data flock traveling hop-by-hop from Source Agent $i$ to Destinations $j$, $k$ and $l$ while avoiding a DoS region. We represent a single multicast packet intended for $D$ destinations as $D$ *flockmates* with identical $(x, y)$ coordinates and distinct $z$-coordinates in the 3-D space as distinguished in Fig. 4.3 via hues of green, magenta and brown stacked in
the $z$-direction. To model multicast packet replication and route separation, the corresponding flockmates would appropriately separate into two partitions in $(x, y)$ space. The reader should note that within this framework unicast routing would reduce to 2-D flocking.

Network nodes are assumed to allow bidirectional multicast communications, be equipped with buffers, and be aware of their queue lengths, number of predecessors processed/dropped in the last $\ell$ time steps and an estimate of the minimum number of hops to a given destination. We assume that route decision-making does not cause significant processing delay.

We next discuss the details of GOAliE in two parts; Section 4.3.1 presents the selection of the next hop in multi-hop routing while Section 4.3.2 focuses on packet replication and route separation of multicast packets.

4.3.1 GOALIE Multi-hop Routing

We predicate that adaptive packet routing under varying network conditions and attack is analogous to behavioral transitions in collective formation within large-scale flocks. It is well known that the survival of animal groups necessitates change from one type of structure to another in response to stimuli. Moreover, the adaptation is informed, in part, through exchange of flockmate experience. Thus, our routing framework employs mechanisms for active packets to exchange experiential data to facilitate informed distributed route decision-making. At each time step, an active packet assesses its candidate next hop neighbors and prioritizes selection based on information from “predecessor” packets and neighboring nodes; we define predeces-
sors for a given packet as the union of the set of flockmates generated at past time instants that are exactly one hop away and the set of flockmates that have just been transmitted from the relay nodes one hop away.

Correspondingly, our model of network dynamics incorporates the states of both relay nodes and packets. Assume the smart grid system is comprised of $D$ agents representing all possible communication sources and destinations. At the time step $k$, we define the state of the $l$th node by $\zeta_l = \{Q_{l,k}, R_{l,k}\}$ where $Q_{l,k}$ is the associated queue length and $R_{l,k} \in \mathbb{R}^D$ denotes a vector whose $j$th element $R_{l,k}(j)$ represents a predecessor experiential estimate of the minimum number of remaining hops from the $l$th node to the $j$th destination agent. Similarly, at time step $k$, we represent the state of an active packet generated at time $k' \leq k$ with Source Agent $i$ and Destination Agent $j$ to be $\chi_{ij}^{k'}(k) = [q_c(k), p_c(k), T_c(k)]$ where $q_c$ is the minimum number of remaining hops to reach Agent $j$, $p_c$ is its “routing velocity” which is a measure of the change (within the last time step) in $q_c$, and $T_c$ is its total hop count used by packets traveling to Destination Agent $i$ to predict their minimum number of remaining hops. Thus, an active packet’s routing dynamics can be described as:

\[
\begin{align*}
    p_c(k) &= u_c(k) \quad \text{(update pkt velocity for route decision)} \tag{4.1} \\
    q_c(k+1) &= q_c(k) + p_c(k) \quad \text{(update remaining hops)} \tag{4.2} \\
    T_c(k+1) &= T_c(k) + 1 \quad \text{(update total # hops traversed)} \tag{4.3}
\end{align*}
\]

where $u_c(k)$ is the effect of the routing strategy measured in terms of the change in number of hops to the destination, which we assign to packet velocity $p_c(k)$. Eqs. 4.2 and 4.3 update the minimum number of hops to Agent $j$ and the running total of number of hops traversed, respectively.

\subsection{4.3.1.1 Goal Seeking Constraint}

We consider an analogy between an active packet’s objective to reach its destination in a minimum number of hops and goal seeking. This suggests that an ideal goal for routing would be to have a packet velocity of $p_c^* = -1$, which implies that at each hop the packet is one hop closer to its destination. However, given the collaborative nature of our routing model, it is necessary to consider routing decisions that optimize other metrics such as the synchronization of other packets and buffer overflow. Thus, we permit our routing strategy to consider candidate next hop neighbors such that $u_c(k) \in \{-1, 0\}$. 
4.3.1.2 Obstacle Evasion

As illustrated in Fig. 4.3, we model a region impacted by DoS or congestion as an obstacle that routing must circumvent. To facilitate informed obstacle evasion, the network nodes and packets exchange state information to communicate the existence of bottlenecks. At time $k$, a packet traversing from Agent $i$ to $j$ that jumps to an intermediate Node $l$ interacts as follows:

\[
R_{l,k}(i) = T_c(k) \quad \text{packet } \xrightarrow{\text{state info}} \text{node},
\]

\[
q_c(k) = R_{l,k}(j) \quad \text{node } \xrightarrow{\text{state info}} \text{packet}.
\]

If more than one packet is traveling from Source Agent $i$ at time $k$, then the minimum $T_c(k)$ will be assigned to $R_{l,k}(i)$. Eq. 4.4 allows Node $l$ to store the minimum hops traveled by packets from Source Agent $i$ for later use by packets traveling to Destination Agent $i$ assuming bidirectional symmetry. Conversely, in Eq. 4.5, Node $l$ updates the packet’s hop distance to Destination Agent $j$ using information it has previously acquired from Agent $j$ source packets. Thus packets that have traversed through a region impacted by a DoS will have the opportunity to make this known to those potentially crossing it from the opposite direction, so routing decisions may be made to evade the bottleneck.

4.3.1.3 Next Hop Selection

The next hop routing decision for a packet at Node $l$ is made by considering all possible candidate host nodes that are one hop away and prioritizing them. Class 1 hosts are those for which candidates have not dropped any predecessors in the last time $\ell$ time instants and have successfully transmitted one or more predecessors. Class 2 hosts are those for which candidates have not dropped any predecessors in the last time $\ell$ time instants but have not successfully transmitted predecessors. Thus, candidates in both Class 1 and 2 have not recently suffered from buffer overflow. Class 3 includes the remaining candidates that have dropped at least one predecessor. Routing is prioritized to hosts in Class 1. If none exist, priority goes to Class 2 and then finally to Class 3. If more than one candidate exists in the highest priority class that has non-zero candidates, then we select amongst them using a strategy that accounts for the likelihood of buffer overflow (equated to collision avoidance) while balancing packet latency (goal seeking).

4.3.1.4 Collision Avoidance

Flockmate collisions are employed as a metaphor for buffer overflow in a node. At time $k$, we compute a collision (overflow) likelihood measure for each packet at Node $l$ traveling from
Agent $i$ to $j$:  

$$
M_t = \frac{\tilde{r}_{a,i} + Q_l - \tilde{r}_{d,j}}{\tilde{r}_{a,i} + Q_l},
$$

(4.6)

where $\tilde{r}_{a,i}$ and $\tilde{r}_{d,j}$ are estimates of the number of packets at Node $l$ arriving from Agent $i$ and leaving Agent $j$, respectively, for time $k$, and $Q_l$ is the queue length of the node at time $k-1$. Eq. (4.6) indicates that at time $k$ a node with smaller $M_t$ has lower likelihood of overflow.

To predict $\tilde{r}_{a,i}$ and $\tilde{r}_{d,j}$ based on predecessor experiences, our scheme employs a Hamming window to temporally weight the predecessor states to provide greater robustness against data outliers:

$$
\tilde{r}_{a,i} = \frac{\sum_{n=1}^{\ell} h(n-1) r_{a,i}(n)^2}{\sum_{n=1}^{\ell} h(n-1)}, \quad \tilde{r}_{d,j} = \frac{\sum_{n=1}^{\ell} h(n-1) r_{d,j}(n)^2}{\sum_{n=1}^{\ell} h(n-1)},
$$

(4.7)

where $r_{a,i}, r_{d,j} \in \mathbb{Z}^{+\ell}$ are, respectively, the vectors containing the numbers of arrivals and departures in the $\ell$ most recent time steps in chronological order, and $h(n)$ is the $\ell$-point Hamming window $h(n) = 0.54 - 0.46 \cos \left( \frac{2\pi n}{2\ell-3} \right)$ giving highest weight to the most current information.

To balance this with low latency objectives for goal seeking, we make use of the following intermediate metric:

$$
d_l = \begin{cases} 
1, & \text{if } R_{l,k}(i) < q_c(k), \\
\gamma, & \text{otherwise},
\end{cases}
$$

(4.8)

where constant $\gamma > 1$ is a penalty parameter for not transmitting the packet closer to Agent $j$, used to compute the desirability of a candidate host as follows:

$$
D_l = \frac{1 - M_l}{d_l},
$$

(4.9)

where a candidate with higher desirability $D_l$ has higher likelihood of routing the packet. This is implemented by first ranking the candidate host nodes according to their $D_l$ value. At each time step and for a packet $v$, a vector $\Upsilon_v$ is created whose elements are the indices of candidate hosts ordered in decreasing desirability. The probability of routing to the $r$th node of the ranked list is assigned geometrically with appropriate normalization factor $\beta$ as follows:

$$
p_r = \beta (1 - \beta)^r, \quad r = 1, 2, \ldots, |\Upsilon_v|
$$

(4.10)

where the parameter $0.5 < \beta \leq 1$ controls the degree of randomization of our routing protocol; a smaller $\beta$ indicates higher randomization and implies greater resilience to DoS or sudden congestion while $\beta = 1$ represents aggressive routing with no randomization.
Thus, this section pertains to next hop selection for flockmates with different \((x, y)\) coordinates. Flockmates with the same \((x, y)\), but different \(z\)-coordinates (modeling a single multicast packet) must decide at each hop whether they must remain together or separate for multicast route splitting, as we discuss next.

### 4.3.2 GOAliE Multicast Routing

Multicast involves communications between a single source and multiple destinations such that a single packet is initially transmitted to save bandwidth until it is decided that the packet must be replicated and split routes to balance individual destination latencies. We address multicast routing through pairwise flockmate attraction and repulsion as a function of the congruence of their destinations.

Consider flockmates \(v\) and \(w\) with the same \((x, y)\)-coordinates and distinct \(z\)-coordinates that represent components of a single multicast packet with different destinations. The multicast dynamics take place in the \(z\)-direction such that flockmates distant along \(z\) are considered to be repelled by one another and enable multicast splitting at the next hop. In contrast, flockmates in close proximity in \(z\) remain together for routing. We characterize the interaction at each time step \(k\) in terms of forces modeled via potential functions \(V_1(k)\) and \(V_2(k)\); the reader is referred to [123] for potential functions in the context of flocking. The associated acceleration between flockmates \(v\) and \(w\) is computed by differentiating the potential function with respect to the relative position vector between \(v\) and \(w\) in the \(z\)-direction.

Let \(\Upsilon_{vw}\) be a vector of length \(L_{vw}\) consisting of elements in \(\Upsilon_v \cap \Upsilon_w\) (representing candidate next hop hosts common to flockmates \(v\) and \(w\)). Each element of \(\Upsilon_{vw}\) is associated with two routing likelihood values \(v_l = [p_{r_1}, p_{r_2}]\), \(l = 1, 2, \ldots, L_{vw}\) (from Eq. 4.9 where \(r_1\) and \(r_2\) represent the rankings in order of decreasing desirability \(D_l\) of candidate host \(\Upsilon_{vw}(l)\)) for flockmates \(v\) and \(w\), respectively. We let \(\nu = [\nu_1, \nu_2, \ldots, \nu_{L_{vw}}]\). A measure of congruency in the individual destination trajectories of flockmates \(v\) and \(w\) is evaluated as:

\[
\zeta_{vw} = \min \left\{ \sum_{l=1}^{L_{vw}} \nu_l(1), \sum_{l=1}^{L_{vw}} \nu_l(2) \right\},
\]

(4.11)

and represents a value for use in modeling multicast flockmate attraction or repulsion.

To determine the nature of interaction between each pair of flockmates \((v, w)\), at time \(k\) and \(z\)-positions \(z_v(k)\) and \(z_w(k)\), respectively, we assign a threshold \(\zeta_{th}\). If \(\zeta_{vw} \geq \zeta_{th}\), we conclude that the two flockmates have similar destination trajectories and are attracted to one another to promote staying in the same multicast group. Otherwise, we conclude the flockmates repel each other.
4.3.2.1 \( \zeta_{vw} \geq \zeta_{th} \)

We model the overall dynamics in the \( z \)-direction using the following potential energy function for time \( k \):

\[
V_1(k) = \sum_{v=1}^{L_{vw}} \sum_{w=1, w \neq v}^{L_{vw}} \frac{b_1}{b_2} \exp \left[ b_2 (\zeta_{vw} - \zeta_{th})(\|z_v(k) - z_w(k)\|_\sigma - \|d^*\|_\sigma) \right] \\
- b_1 \times (\zeta_{vw} - \zeta_{th}) (\|z_v(k) - z_w(k)\|_\sigma - \|d^*\|_\sigma),
\]

where \( \| \cdot \|_\sigma \) denotes the \( \sigma \)-norm defined as: \( \| x \|_\sigma = \frac{1}{\sqrt{1 + \epsilon \| x \|}} - 1 \), and \( \epsilon, b_1, \) and \( b_2 \) are positive parameters. Eq. 4.12 enables flockmate attraction without collision; a weak repulsive force is experienced when flockmate separation reaches \( d^* \). The larger the value of \( \zeta_{vw} - \zeta_{th} \), the stronger (weaker) the attraction (repulsion) force. The associated acceleration at time \( k \) is:

\[
g_{v,1}(k) = b_1 \sum_{w=1, w \neq v}^{L_{vw}} (\zeta_{vw} - \zeta_{th}) (\exp[b_2 (\zeta_{vw} - \zeta_{th})]\|z_v(k) - z_w(k)\|_\sigma - \|d^*\|_\sigma) - 1 \}
\]

where \( n_{vw} = \frac{z_v(k) - z_w(k)}{\sqrt{1 + \epsilon \| z_v(k) - z_w(k) \| ^2}} \). Moreover, flockmates that belong to the same multicast group, interact to achieve velocity alignment. This is modeled as a distributed consensus problem [123] in which the flockmates are the vertices of a dynamic graph whose interaction to achieve alignment is determined by the graph’s edge weight. The associated adjacency matrix elements are set to \( a_{vw}(k) = 1 \) if \( \zeta_{vw} \geq \zeta_{th} \) and \( a_{vw}(k) = 0 \) otherwise. The corresponding acceleration is given by:

\[
g_{v,2}(k) = b_3 \sum_{w=1, w \neq v}^{L_{vw}} a_{vw}(k)(\| \bar{v}_v(k) - \bar{v}_w(k) \|),
\]

where \( \bar{v}_v(k) \) is flockmate velocity along the \( z \)-direction (see Eq. 4.17).

4.3.2.2 \( \zeta_{vw} \leq \zeta_{th} \)

We consider the following potential energy function for repulsion:

\[
V_2(k) = \sum_{v=1}^{L_{vw}} \sum_{w=1, w \neq v}^{L_{vw}} \frac{b_4}{2 a_{vw}(k)} (\zeta_{th} - \zeta_{vw})(\|z_v(k) - z_w(k)\|_\sigma - \|d_r\|_\sigma)^2
\]

where \( a'_{vw}(k) = 1 \) for \( z_v(k) - z_w(k) < d_r \) and \( a'_{vw}(k) = 0 \) otherwise. Here, the repulsion decreases to 0 as the flockmate distance increases to a predefined distance \( d_r \). The larger the value of non-congruency \( (\zeta_{th} - \zeta_{vw}) \), the stronger the repulsive force. The acceleration
corresponding to $V_2(k)$ is therefore

$$g_{e,3}(k) = b_4 a^\prime_{uw} (\zeta_{th} - \zeta_{vw}) \sum_{w=1, w\neq v}^{L_{vw}} (\|z_v(k) - z_w(k)\|_\sigma - \|d_r\|_\sigma) n_{vw}. \quad (4.16)$$

### 4.3.2.3 Multicast Dynamics and Decision-Making

The overall dynamics for the $v$th flockmate in the $z$-direction is:

$$\begin{align*}
\hat{v}_v(k + 1) &= \hat{v}_v(k) + \Delta t \sum_{l=1}^{3} g_{v,l}(k), \\
\hat{z}_v(k + 1) &= \hat{z}_v(k) + \Delta t \bar{v}_v(k),
\end{align*} \quad (4.17)$$

where $\Delta t$ is the time between two consecutive time steps.

At each time step $k$, flockmates of the same multicast packet (from Source Agent $i$) cluster into $J_{n,i}$ subgroup(s) at a Node $n$; a cluster algorithm such as [173] is used. If $J_{n,i} > 1$ let $\chi_m$ represent the set of common candidate hosts for flockmates in subgroup $m$ and $W_m$ be their set of destination agent indices. We assign the desirability for a Candidate Host $l$ as $\bar{D}_l = \max_{j \in W_m} \{R_{l,k}(j)\}$. We next rank the elements of $\chi_m$ in decreasing value of $\bar{D}_l$ and assign a probability from Eq. 4.10 to obtain the expected remaining hops (for all subgroup flockmates to reach their destinations) if the group of packets is split into subgroups:

$$R_m = \sum_{r=1}^{||\chi_m||} p_r \bar{D}_{m,r} \quad (4.18)$$

where $r$ denotes the ranking of the candidate host node in $\chi_m$.

Alternatively, we next assume no subgroup splitting and obtain the corresponding set $\tilde{\chi}_i = \bigcap_{m=1}^{J_{n,i}} \chi_m$ consisting of the indices of common candidate hosts for all the members in the multicast group. Similarly, we define $\tilde{D}_l = \max_{j \in \tilde{W}} \{R_{l,k}(j)\}$ where $\tilde{W} = \bigcup_{m=1}^{J_{n,i}} W_m$, and rank the elements in $\tilde{\chi}_i$ in increasing value of $\tilde{D}_l$. For each element of the reordered vector, we assign a probability from Eq. 4.10 and compute the expected number of minimum remaining hops assuming all flockmates stay in the same multicast group at time $k$:

$$\tilde{R} = \sum_{r=1}^{||\tilde{\chi}_i||} p_r \tilde{D}_r \quad (4.19)$$

where $r$ denotes the ranking of the candidate host node in $\tilde{\chi}_i$.

At each time step, the splitting of flockmates within the same multipath group into $J_{n,i}$ subgroups may reduce end-to-end latency (or hop count), but will increase bandwidth (BW)
consumption by \((J_{n,i} - 1)\) units. In order to balance these competing objectives, we define the following cost:

\[
f(n,i) = w_1 \underbrace{J_{n,i} - 1}_{\text{BW metric} > 0} + (1 - w_1) \underbrace{\left(\max_{m=1}^{J_{n,i}} \{R_m\} - \bar{R}\right)}_{\text{latency metric} < 0},
\]

(4.20)

where parameter \(w_1 \in [0,1]\); here \(w_1 = 0\) optimizes latency alone while \(w_1 = 1\) solely considers bandwidth consumption. Thus, at each time step, the group of packets decide whether to split into \(J_{n,i}\) subgroups if \(f(n,i) < 0\). Otherwise they stay together. As soon as the subgroups separate, one packet in each subgroup normalizes its \(z\)-coordinate value to 0.

### 4.4 Simulations and Performance Assessment

Our simulations assess the performance of GOAliE using traditional communication performance metrics including packet delivery ratio and end-to-end latency. In addition, we evaluate GOAliE in the context of a critical smart grid distributed control application [4], maintaining smart grid stability in the face of fault(s) using wide area PMU data. Such a setting illustrates the performance and resilience of routing when the need for data is most critical for power system operation. The performance of our multicast routing approach is compared to a unicast version formerly proposed by the authors [5] and the multicast routing technique, MANSI, based on swarm intelligence [6]. Although MANSI is not designed specifically for smart grid communications routing, it aims for similar adaptive multicast characteristics as GOAliE providing an assessment of the advantage of using a flocking paradigm in particular.

We consider the New England 39-bus test power system of Fig. 4.1 as our underlying physical power system and employ the mesh network of Fig. 4.2 for communications; the mesh network has a uniform grid topology consisting of 61 nodes marked with their corresponding node indices in Fig. 4.2. The buffer capacity of each node is set to 5, network link bandwidth to 200 pkts/sec and the PMU sampling rate to 100 and 200 packets/sec for low and higher congestion scenarios, respectively. In addition, we assign parameters \(\epsilon = 1, b_1 = 1, b_2 = 5, b_3 = \frac{1}{2}, b_4 = 3\) and \(\ell = 5\). To guarantee efficiency in maintaining the smart grid stability, we set the strict end-to-end deadlines to be 0.05 s. We assume in the face of a fault, the associated information needed to maintain smart grid stability has highest priority amongst all communication network information flows. MATLAB/Simulink is employed for simulations.
4.4.1 Case Study I

A 3-phase short circuit fault occurs on the Bus 14 of Fig. 4.1 at time $t = 0$ s. The associated Line 14 – 15 is removed at $t = 0.3$ s, post critical clearing time. The system behavior is illustrated in Fig. 4.4 over a period of 10 s and, as expected, stability is lost as the normalized frequencies, phase angles and phase angle differences diverge beyond operating limits.

![Figure 4.4: (a) Normalized rotor frequencies and (b) phase angles versus time without wide area monitoring and control.](image)

When our proposed distributed control approach is applied, post-fault clusters are first identified as $\{G_1\}$, $\{G_2, G_3\}$, $\{G_4, G_5, G_8, G_{10}\}$, and $\{G_6, G_7, G_9\}$ (at time $t = 0.35$ s) with lead agents selected as $i = 1, j = 3, h = 4$, and $s = 9$ that must communicate through the network of Fig. 4.2. Cyber control is assumed to be activated at $t = 0.38$ s which requires real-time communications and control computation for each lead agent.

The GOAliE parameters $\gamma$ designed to control “greediness” and $\beta$ designed to control “randomization” of the multi-hop protocol are varied. Fig. 4.5 presents the packet delivery ratio for varying of $(\gamma, \beta)$. Fig. 4.5 (a) and (b) shows results for low and higher congestion, respectively, and Fig. 4.5 (c) and (d) considers when congestion is low but DoS attacks are present starting at $t = 5$ s at Node 39 and at Nodes 5 and 6, respectively. For all cases, we set $w_1 = 0.55$ (of Eq. 4.20). As observed, when no DoS is present lower randomization improves performance while $\gamma$ has negligible influence. In the face of DoS, effectively increasing $\beta$ and selected $\gamma$ can improve the networks resilience to attack. For instance, $(\gamma, \beta) = (3, 0.95)$ provides good performance for both DoS cases.

For the same test conditions as Fig. 4.5 and for $(\gamma, \beta) = (3, 0.95)$, Fig. 4.6 presents the packet delivery ratio versus $w_1$. As observed, to ensure resilience to the congestion, $w_1 \geq 0.5$ is needed. Furthermore, to ensure robustness to the DoS attack, $w_1 \leq 0.6$. Therefore, we set $w_1 = 0.55$ to address both classes of bottlenecks.
Figure 4.5: GOAliE packet delivery ratio versus $\gamma, \beta$ for a) low congestion, b) higher congestion, c) DoS attack at Node 39 for $t \geq 5$ s, and d) DoS attack at Nodes 5 and 6 for $t \geq 5$ s.
Figure 4.6: GOAliE packet delivery ratio versus $w_1$ for a) low congestion, b) higher congestion, c) DoS attack at Node 39 for $t \geq 5$ s, and d) DoS attack at Nodes 5 and 6 for $t \geq 5$ s.
We next study end-to-end delay. Once again we focus on the situations of low and higher congestion and DoS attacks on Node $39 \ (t \geq 5 \ s)$, and on Nodes $5$ and $6 \ (t \geq 5 \ s)$. Parameters are set to $(\gamma, \beta) = (3, \ 0.95)$ and $w_1 = 0.55$ for all cases. Figures 4.7 and 4.8 demonstrates how there is a natural adaptation stage at the beginning of communications in which experience is initially propagated amongst flockmates to improve performance. This also occurs amidst DoS to improve delay. Overall, we conclude that adaptation enables latency improvements within a few seconds.

![High Congestion](image1.png)

High Congestion

![DoS Attack at Node 39](image2.png)

DoS Attack at Node 39

![DoS Attack at Nodes 5 and 6](image3.png)

DoS Attack at Nodes 5 and 6

Figure 4.7: GOAliE end-to-End Latency versus packet generating time for a) higher congestion, and b) DoS attack at Node 39 for $t \geq 5 \ s$.

Figure 4.8: GOAliE end-to-End Latency versus packet generating time for DoS attack at Nodes 5 and 6 for $t \geq 5 \ s$.

Figs. 4.9 to 4.12 compare the performance of GOAliE with existing routing protocols [5, 6]. To assess performance in the context of a smart grid application, the effectiveness of the routing approach for wide area communications for the distributed control scenario of [4] is considered.
In Figs. 4.9 and 4.10, we consider high congestion and a PMU packet rate of 200 packets/sec. We compare our proposed multicast routing scheme with the unicast version of [5] to observe that multicast routing efficiently improves resilience to high congestion, which has a beneficial effect for real time control as witnessed by the greater stabilization of frequency.

In Figs. 4.11 and 4.12, we consider DoS attack at Nodes 5 and 6 for $t \geq 5$ s. The PMU packet rate is set to 100 packets/sec for low congestion. We compare GOAliE to MANSI [6] and observed that our proposed approach is still more resilient to DoS attack by predicting the impacted network region in real-time and adaptively routing packets.

![Figure 4.9](image1.png)  
**Figure 4.9:** (a) Normalized rotor frequencies and (b) phase angles versus time in the presence of distributed control [4] for high congestion by using GOAliE

![Figure 4.10](image2.png)  
**Figure 4.10:** (a) Normalized rotor frequencies and (b) phase angles versus time in the presence of distributed control [4] for high congestion by using the unicast routing scheme [5].
Figure 4.11: (a) Normalized rotor frequencies and (b) phase angles versus time in the presence of distributed control [4] for DoS by using GOAliE.

Figure 4.12: (a) Normalized rotor frequencies and (b) phase angles versus time in the presence of distributed control [4] for DoS by using MANSI multicast routing [6].
4.4.2 Case Study II

We assume that a 3-phase short circuit fault occurs on the Bus 21 of Fig. 4.1 at \( t = 0 \) s and that the associated Line \( 21 - 22 \) is removed at \( t = 0.3 \) s, post critical clearing time. The system behavior without control is shown in Fig. 4.13 over a period of 10 s and, as expected, stability is lost.

When the proposed distributed control approach is applied, post fault clusters are identified as \( \{ G_1, G_{10} \} \), \( \{ G_2, G_3, G_4, G_5, G_8, G_9 \} \), and \( \{ G_6, G_7 \} \) at \( t = 0.35 \) s with lead agents selected as \( i = 1, j = 4 \), and \( h = 6 \) that communicate through the multi-hop mesh network in Fig. 4.2 for real-time control beginning at \( t = 0.38 \) s.

![Figure 4.13: (a) Normalized rotor frequencies and (b) phase angles versus time without wide area monitoring and control.](image)

Fig. 4.14 presents the GOAliE routing packet delivery ratio for varying \((\gamma, \beta)\) under low and higher congestion, and DoS attacks at Node 21 and at Nodes 27 and 28 both starting at \( t = 5 \) s. As observed, when DoS is not present lower degrees of randomization via parameter \( \beta \) improves performance while the penalty \( \gamma \) has negligible influence. For DoS, effectively increasing \( \beta \) and selecting \( \gamma \) can improve the network’s resilience to attack. For instance, \((\gamma, \beta) = (3, 0.95)\) provides good performance for both DoS cases.

We next study the effect of the end-to-end delay on the ability of distributed control to maintain smart grid stability. Once again we focus on higher congestion and DoS attacks on Node 21 and on Nodes 27 and 28 both for \( t \geq 5 \) s. Parameters were consistently set to \((\gamma, \beta) = (3, 0.95)\) and \( w_1 = 0.55 \). Figures 4.15 and 4.16 demonstrate the successful performance of the routing protocol under both high congestion and DoS. The adaptation improves latency in the presence of network bottlenecks within a few seconds.

Figure 4.17 evaluates multicast routing performance for distributed control [4] of the New England 39-bus power system. We consider high congestion and DoS attack at Nodes 5 and 6.
Chapter 4. GOAliE: A Resilient Multicast Routing Approach in Smart Grids

Figure 4.14: GOAliE packet delivery ratio versus $(\gamma, \beta)$ for a) low congestion, b) higher congestion, c) DoS attack at Node 21 for $t \geq 5$ s, and d) DoS attack at Nodes 27 and 28 for $t \geq 5$ s.

Figure 4.15: GOAliE end-to-end latency versus packet generating time for a) higher congestion, and b) DoS attack at Node 21 for $t \geq 5$ s.
Figure 4.16: GOAliE end-to-end latency versus packet generating time for DoS attack at Nodes 27 and 28 for $t \geq 5$ s.

Figure 4.17: Normalized rotor frequencies and phase angles versus time for distributed control [4] for GOAliE: (a) and (b) in the face of high congestion and (c) and (d) DoS attack.
for $t \geq 5$ s with parameters $(\gamma, \beta) = (3, 0.95)$ and $w_1 = 0.55$. The PMU packet rate is 200 packets/sec for high congestion and 100 packets/sec for low congestion. It is clear from the generators’ performance that smart grid stability is maintained in the presence of serious fault on the Bus 21 through both high congestion, and DoS attack, thus demonstrating the potential of proposed adaptive multicast routing strategy.

4.5 Conclusions

In this chapter, we propose an adaptive distributed multicast approach for PMU communication routing in multi-hop mesh networks for wide area monitoring and control. We model interactions amongst network packets in terms of local optimizations and/or pairwise “forces” based on flocking theory. We assert that such an approach provides a convenient methodology for development of an adaptive distributed and resilient multicast routing technique. Although our selections of decision-making metrics and potential functions are not unique, they are designed to facilitate computation and resilient selection through effective monotonic parameter trends, rank order and/or the appropriate incorporation of competing objectives.

We observe the advantages of goal seeking, obstacle evasion, collision avoidance and behavioral transitions strategies from flocking for timely and resilient distributed multicast data delivery in comparison to existing routing techniques. We conclude that our distributed multicast routing approach, which that makes use of predecessor packet experiences much like flocks in nature, has the potential to facilitate an adaptive, self-healing and resilient communications in smart grid applications. Our framework conveniently represents communication dynamics in a form that can be integrated with power system dynamics to provide a comprehensive framework for understanding cyber-physical system interactions.
Chapter 5

Conclusions

5.1 Summary and Conclusions

The last few years have witnessed the radical transformation in structure and functionality of electrical energy systems. Such systems were traditionally executed in the physical world and are now also cyber-enabled. This cyber-enabled energy system, called smart grid, can be envisioned as the marriage of information technology with the electricity network. While its increased dependence on cyber infrastructure aims to enable greater reliability, efficiency and capacity of power delivery, this reliance also creates a host of unfamiliar vulnerabilities. Due to the highly integrated and connected nature of smart grids, it is important to account for their salient cyber-physical coupling when making critical design decisions and identifying solutions to promote security.

In this dissertation, our research focuses on developing a flocking-theory inspired dynamical systems paradigm to model smart grid cyber-physical interactions related to smart grid stability. Such a biologically-inspired framework enables the convenient description of (discrete) cyber and (analog) physical couplings. Through this paradigm, we demonstrate real-time cyber-physical integrated control and communication strategies using “wisely”-placed phasor measurement units and energy storages to re-stabilize a smart grid system under various forms of cyber and physical attacks.

Our research has evolved in three stages. We first propose a multi-agent dynamical systems paradigm to model the cyber-physical interactions related to smart grid stability. In our multi-agent framework each node, representing both electrical and information system components, is modeled as having dynamics that synergistically describe physical and information couplings with neighboring agents. Inspired by the analogy between the flocking behavior in the nature and the stability of the cyber-enabled synchronous generators, We develop a flocking-based scheme to formulate the cyber-physical integrated action for each agent. It
is clear from our analysis framework that redundant cyber information acquisition and use increases risks of cyber-attack whereby indiscriminate cyber-dependence and -connectivity increases attack scope and impact. To address this problem, in the second stage, we extend the multi-agent paradigm to a two-tier hierarchical framework by effectively leveraging physical couplings between the agents and identifying the critical ones that increase vulnerability to cyber- or physical-attack. With the developed hierarchical framework, the cyber information redundancy is reduced by only leveraging cyber coupling at critical agents. In the context of the hierarchical framework, we analyze the physical impact of cyber attack. We focus on two major attacks widely effecting the smart grid, attacks on timely data delivery, such as Denial-of-Service (DoS) attacks, and attacks on information accuracy, such as false data injection attacks. The DoS attack can cause communication delay of critical cyber information and result in significant power delivery disruption. To mitigate the DoS attacks, we propose an intelligent multicast routing strategy, called Goal-Seeking Obstacle and Collision Evasion (GOALiE), which is appropriate to smart grids and resilient to DoS attacks. We also develop a novel witness-based cyber-physical protocol whereby physical coherence is leveraged to probe and identify the false data injection on PMU data and estimate the true information values for attack mitigation.

5.2 Contributions

1. The proposed flocking-based dynamical systems paradigm for smart grid analysis is one of the first applications to address the interaction between the cyber information flow and physical power flow in smart grids. This work is also one of the first applications of the graph-based dynamical system methodology and the biologically inspired multi-agent system cooperative control methodology to address the cyber-physical security issues for smart grids.

2. The developed two-tier hierarchical cyber-physical framework successfully harnesses physical couplings within a power system to facilitate the selective use of cyber data acquisition and distributed control, which enables the identification of large-scale distributed control strategies for robust and resilient smart grid operation.

3. The proposed multi-flock-based generator coherency identification technique successfully realizes the real-time detection of generator coherency within a short observation window even in the measurement environment with white noise or information corruption. Besides being used in the proposed hierarchical cyber-physical control framework, the proposed generator coherency identification method is believed to establish itself as
an important tool to aid in the other applications of resistance of cascading failures within wide-area power systems.

4. The proposed witness-based security protocol efficiently identify and mitigate information corruption in smart grid systems by taking a hierarchical cyber-physical perspective and effectively leveraging the telltale physical couplings within the system.

5. The proposed QoE-based resilient multicast routing approach, GOALiE, provides insight on effective multicast routing principles to promote resilience in faulted power systems in the presence of congestion and denial-of-service attacks on communications infrastructure, which exhibits the potential to facilitate an adaptive, self-healing, and resilient communications infrastructure for smart grids. This approach also conveniently represents communication dynamics in a form that can be integrated with power system dynamics to provide a comprehensive framework for understanding cyber-physical system interactions.

5.3 Future Research

For the continuation of our current work, we plan to focus on the following research directions in the future:

1. The principles of our flocking-based hierarchical cyber-physical security framework can be applied to small-scale smart grids, such as Microgrids which employ a large number of distributed generators and intermittent energy resources like solar and wind. We believe that the proposed framework exhibits the potential to facilitate a cyber-physical control strategy for Microgrids under severe disturbance.

2. The work of resilient multicast routing approach can be extended to achieve an adaptive and self-healing communication infrastructure for smart grids. This work can also be continued to analyze the integration of communication dynamics and power systems dynamics and design smart grid strategies for overall system resilience to cyber and physical disruption.

3. A generalized cyber-physical intrusion detection protocol can be derived based on the work of witness-based security protocol.

4. Smart grid represents a rich and challenging case study to craft cyber-physical system analysis and synthesis tools. The results achieved for smart grids can be used to develop fundamental insights for the design of robust and secure cyber-physical systems.
A graph $G$ is specified by a vertex set $\mathcal{V} = \{1, 2, \ldots, N\}$ and an edge set $\xi = \{(i, j) : i, j \in \mathcal{V}, j \neq i\}$ whose elements characterize the incidence relation between distinct pairs of $\mathcal{V}$ [174, 175]. Two vertices $i$ and $j$ are called adjacent when $(i, j) \in \xi$. The graph $G$ is said to be undirected if $(i, j) \in \xi \iff (j, i) \in \xi$. The quantities $N$ and $|\xi|$ are called order and size of the graph. For the networked dynamic systems, $|\xi|$ is called the communication complexity of the system [176].

We can associate a matrix with each graph storing some of the information about the graph in that matrix. This matrix can be used to obtain more detailed information about the graph. If a graph has $N$ vertices, we may associate an $N \times N$ matrix $A = [a_{ij}]$ which is called adjacency matrix. The vertex matrix $A$ is a matrix with nonzero elements satisfying the property $a_{ij} \neq 0 \iff (i, j) \in \xi$. The graph is called weighted whenever the elements of its adjacency matrix are other than just $0 - 1$ elements. Here, we mostly use weighted graphs with position-dependent adjacency elements. For an undirected graph $G$, the adjacency matrix $A$ is symmetric, i.e. $A^T = A$. The set of neighbors the $i$th node is defined as follows:

$$\mathcal{N}_i = \{j \in \mathcal{V} : a_{ij} \neq 0\} = \{j \in \mathcal{V} : (i, j) \in \xi\}. \quad (A.1)$$

The adjacency matrix $A$ is a fundamental matrix which is used to define other important matrices associated with the same graph. For example, the degree matrix $D = [d_{ij}]$ is defined by using the corresponding adjacency matrix $A$ as follows:

$$d_{ij} = \begin{cases} \sum_{k=1}^{N} a_{ik}, & \text{if } i = j; \\ 0, & \text{if } i \neq j. \end{cases} \quad (A.2)$$

The Laplacian Matrix $L$ can be calculated by the corresponding adjacency matrix $A$ and
degree matrix $D$ as follows:

$$L = D - A. \quad (A.3)$$
Appendix B

Spectral Matrix-based Coherency Identification Method

In this chapter, we propose an alternative generator coherency identification technique, a special matrix-based approach.

B.1 Coherency Identification Method

We exploit the fact that the matrix $L$ can be interpreted as the a Laplacian of a directed weighted graph $G$ associated with the power system topology for a small time interval after the disturbance is cleared; the associated weight of an edge $e_{ij}$ in $G$ would be given by $l_{ij}$ of Eq. (3.4). It is well known that for Laplacian matrices, the second smallest eigenvalue $\lambda_2$ represents the algebraic connectivity of its associated graph. Moreover, for our framework the signs of the elements of the associated eigenvector $v$ (called the Fiedler vector) provide information for spectral bisection [177, 178] to partition $G$ into two relatively disjoint subgraphs in terms of physical coupling.

An algorithm to identify agent coherency is summarized in Table B.1. Our proposed algorithm is able to adaptively determine the appropriate number of clusters. The algorithm is fault-dependent and real-time so that it can be applied shortly after a system fault is cleared to analyze coherency just prior to the application of control. After identification of coherent clusters, the two-tier hierarchical controlling framework described in the next section is applied.

As described, for each cluster, we compute the vector $\sigma_{+(-)}$, which represents the distance between the states of the agents and the weighted cluster “center.”
Table B.1: Spectral Matrix-Based Agent Coherency Identification Method

1. Obtain the Laplacian matrix \( L \) by using Eq. (3.4).
2. Calculate the eigenvector \( \mathbf{v}_s \) corresponding to the smallest nontrivial eigenvalue of the Laplacian matrix.
3. For \( k = 1 : N \)
   - if the \( k \)th element of the eigenvector \( \mathbf{v}(k) > 0 \)
     - the \( k \)th agent belonging to the partition \( S^+ \),
   - else
     - the \( k \)th agent belonging to the partition \( S^- \),
   end

4. Let \( I_+ \) and \( I_- \) be the index set of the agents belonging to \( S^+ \) and \( S^- \), respectively,
   1). Calculate:
   \[
   \beta_+ = \frac{\sum_{k \in I_+} \mathbf{v}_s(k) M_k}{\sum_{k \in I_+} M_k},
   \sigma_+ = \frac{\mathbf{v}_s - \beta_+}{\beta_+},
   \]
   where \( M_k \) be the inertia of the generator being to the \( k \)th agent.
   2). If \( \exists |\sigma_+(k)| > 0.5 \), continue to partition \( S^+ \). The subpartition \( S^+_n \) consists
   of the agents whose corresponding element of \( \exists \sigma_+ \) locates within the range \([n - 0.5, n + 0.5]\), where \( n = 0, \pm 1, \cdots \).
   3). Similarly, calculate \( \beta_- \), \( \sigma_- \), and \( \zeta_- \) for the agents belonging to \( S^- \) and
   continue to partition \( S^- \) if \( \exists |\sigma_-(k)| > 0.5 \).

B.2 Case Study

We demonstrate the performance of our flocking-based two-tier hierarchical control framework in achieving smart grid stability for two case studies on the 5-generator, 14-bus power system of Fig. B.1 which is a modified version of IEEE 14-bus power system; modifications are listed in Table B.2, and the generator data used in the dynamic analysis is listed in Table B.3. MATLAB/Simulink is employed for simulations.

The system disturbance consists of a 3-phase short circuit at Bus 4 of Fig. B.1 which occurs at time \( t = 0 \) s. The line 4 – 5 is removed at \( t = 55 \) ms. Fig. B.2 shows the normalized rotor

<table>
<thead>
<tr>
<th>Modified Buses</th>
<th>IEEE 14-Bus System</th>
<th>Our Test System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bus 3</td>
<td>Synchronized Condenser With Power 0+23.39357i</td>
<td>Synchronized Generator With Power 20+23.39357i</td>
</tr>
<tr>
<td>Bus 6</td>
<td>Synchronized Condenser With Power 0+12.24036i</td>
<td>Synchronized Generator With Power 30+12.24036i</td>
</tr>
<tr>
<td>Bus 8</td>
<td>Synchronized Condenser With Power 0+17.3566i</td>
<td>Synchronized Generator With Power 50+17.3566i</td>
</tr>
</tbody>
</table>
frequencies and phase angle differences over a period of 20 s. We observe that the generator coherency involving the following groups: \( \{G_1, G_2, G_3\} \), \( \{G_4\} \) and \( \{G_5\} \).

The implementation of the spectral matrix based agent coherency identification algorithm is completed at \( t = 0.65 \) s. Here, based on the information obtained by PMUs, we compute the
Laplacian matrix $L$, eigenvalue $\lambda_2$ and associated Fiedler vector $v$ as follows:

$$
L = \begin{pmatrix}
5.7061 & -3.0942 & -1.1897 & -1.0004 & -0.4218 \\
-3.0938 & 6.2324 & -1.6636 & -0.9325 & -0.5424 \\
-1.1860 & -1.6640 & 4.0536 & -0.5673 & -0.6363 \\
-0.9997 & -0.9314 & -0.5688 & 3.2142 & -0.7144 \\
-0.4219 & -0.5363 & -0.6254 & -0.7154 & 2.2990
\end{pmatrix}, \quad (B.1)
$$

$$
\lambda_2 = 2.8460,
$$

$$
v = [-0.2895, -0.2655, -0.2327, -0.1025, 0.8838]^T.
$$

Based on the signs of the elements of the eigenvector $v$, we achieve the partitions $S^+ = \{G_1, G_2, G_3, G_4\}$ and $S^- = \{G_5\}$. For Partition $S^+$, we calculate the weighted center value $\beta_+ = -0.2334$ and state-distance vector $\sigma_+ = [0.241, 0.138, -0.003, -0.561]^T$. Since $\sigma_+(4) > 0.5$, we continue to partition $S^+$ and obtain the subpartitions: $S_0^+ = \{G_1, G_2, G_3\}$ and $S_{-1}^+ = \{G_4\}$. For the subpartition $S_0^+$, $G_3$ has the corresponding element with the smallest absolute value, and hence is selected as the lead agent. Therefore, we conclude that there are three clusters $\{G_1, G_2, G_3\}$, $\{G_4\}$ and $\{G_5\}$. 
Bibliography


[66] H. Hadeli, R. Schierholz, M. Braendle, and C. Tuduce, “Generating configuration for missing traffic detector and security measures in industrial control systems based on


[160] K. Kumar1, M. Radhakrishnan, K. Sivalingam1, D. Seetharam, and M. Karthick, “Comparison of publish-subscribe network architectures for smart grid wide area monitoring,”


