Biologically Inspired Hierarchical Cyber-Physical Multi-agent Distributed Control Framework for Sustainable Smart Grids

Jin Wei and Deepa Kundur

Abstract. It is well known that information will play an important role in enhancing emerging power system operation. However, questions 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 cyber attack whereby indiscriminate cyber-dependence and -connectivity increases attack scope and impact. In this chapter, we present a hierarchical cyber-physical framework of power system operation based on flocking theory in the context of the smart grid stability problem. We study strategies to harness an appropriate degree of cyber technology by effectively leveraging physical couplings. Our formulation enables the identification of large-scale distributed control strategies for robust power grid operation. Furthermore, our formulation also enables 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.

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 [25]. The electric power grid

Jin Wei
Department of Electrical and Computer Engineering, The University of Akron, Akron, OH 44325, USA
e-mail: jwei1@uakron.edu

Deepa Kundur
Department of Electrical and Computer Engineering, University of Toronto, The Edward S. Rogers Sr., Toronto, ON M5S 2E4, Canada
e-mail: dkundur@comm.utoronto.ca

S.K. Khaitan, J.D. McCalley, and C.-C. Liu (eds.), *Cyber Physical Systems Approach to Smart Electric Power Grid*, Power Systems, DOI: 10.1007/978-3-662-45928-7_9

started in 1896, based in part on Nikola Tesla's design published in 1888 [58]. 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 [48, 74, 77]. 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 [6]. 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 [11, 103]. 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 [44]. 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 [5]. 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 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 [2].

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, 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 [4, 45]. 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 [50, 111]. 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 [60]. 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 [40, 113]. 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 [28, 59, 66, 83, 87, 121]. 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) [52], the document Roadmap to Achieve Energy Delivery System Cyber Security released by the DOE [3], and Critical Infrastructure Protection (CIP) standards proposed by the NERC [1]. 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 Prior Art

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 [8, 12, 14, 16, 18, 19, 24, 29, 31, 35, 38, 41–43, 47, 53, 55–57, 61, 62, 67–71, 86, 90, 91, 97, 98, 100, 104, 107, 112, 114, 118, 122]. 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 [10].

Research focused on cyber security often takes an information-centric perspective in which data protection is of paramount importance [23]. 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 [68]. 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 [8, 12, 14, 16, 18, 19, 24, 29, 31, 35, 38, 41–43, 47, 53, 55–57, 61, 62, 67–71, 86, 90, 91, 97, 98, 100, 104, 107, 112, 114, 118, 122]. 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 [32, 89]. 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 [73, 82, 84, 85, 93, 94].

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 [26, 63, 64, 81, 110] to relate one or more cyber attacks to one more 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 [36, 36, 38, 54, 80, 101, 106] 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 [17, 17, 51, 88, 108, 109]. Similarly, such contextual information relating cyber and physical dependencies have been exploited for intrusion detection [27, 27, 72, 105, 119, 120]. Testbed systems research addresses the exploration of practical vulnerabilities through SCADA testbed development and construction [30, 33, 46]. 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 [9, 20, 21, 21, 22], which focuses on how data corruption of denial of information access can affect the control of the power grid. Finally, the research in [75,76] represented a work in progress towards the development of a comprehensive and practical framework for electric smart grid cyber attack impact analysis.

1.3 Methodology and Motivation of Biologically Flocking-Based Perspective

As illustrated in Fig. 1, in order to achieve our research objectives, we make use of the tool-sets consisting of graph theory, dynamical-system formulation, and flocking rules. A graph is defined by a collection of vertices (also called nodes) and a

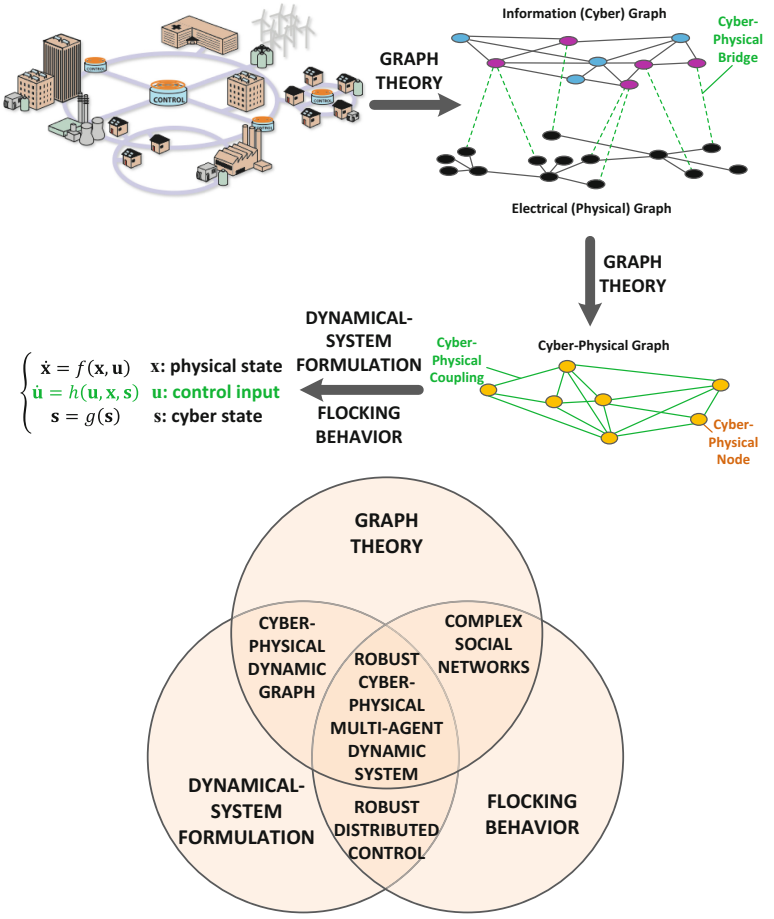


Fig. 1 Methodology overview: tool-sets consisting of graph theory, dynamical-system formulation, and flocking rules

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 [37, 39, 54]. However, as stated in [39], 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, $\mathbf{x}$ denotes the physical state of the system. Because of the physical characteristics of power system, the time-evolution of $\mathbf{x}$ is described by the following differential equation:

$$\dot{\mathbf{x}} = f(\mathbf{x}, \mathbf{u}),$$

where $\dot{\mathbf{x}}$ is the time-derivative of $\mathbf{x}$, $\mathbf{u}$ 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, $\mathbf{s}$ in Fig. 1 represents the cyber measurement of the system and the measurement function $g(\cdot)$ in our work is formulated as follows:

$$g(\mathbf{s}) = \mathbf{s} + \mathbf{n},$$

where $\mathbf{n}$ 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, in the graph, the state change of each cyber-physical node can be formulated by a dynamic function $f(\cdot)$ of the physical state $\mathbf{x}$ and the cyber-physical control input $\mathbf{u}$. 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 $\mathbf{s}$ and the proposed cyber-physical control protocol achieving $\mathbf{u}$, 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.

1.4 Contributions

In this chapter, we propose a flocking-based hierarchical cyber-physical security analysis framework which incorporates cyber intelligence and control behaviors by taking a *flocking* perspective commonly used to model large-scale natural phenomenon. We assert that our framework 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. Fourth, the analogy between the dynamics of synchronous generators and the flocking behavior in the nature enables the exploration on 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 cyber information can benefit scalability and robustness to information attack. 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. We also 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. Furthermore, 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.

This chapter is organized in the following sections. In Section 2, we introduce a dynamic multi-agent system framework on cyber-physical integration modeling for the application of smart grid stability maintenance. A hierarchical control protocol design inspired by the analogy to flocking behavior is proposed in Section 3. Our proposed timely dynamic agent coherency identification for achieving hierarchy is briefly introduced in Section 4. In Section 5, we develop a witness-based verification and estimation protocol for detection and mitigation of information corruption on critical PMU data. The performance is evaluated in Section 6 and the conclusions are provided in Section 7.

2 Dynamic Multi-agent System Framework for Cyber-Physical Integration Modeling

In our research, we consider the smart grid stability from the power system (physical) perspective, which derives from standard control stability [78] and can be seriously impacted by the cyber-physical interactions in the system. In contrast to the control stability, 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 disturbance, with all system variables bounded so that system integrity is preserved [78, 79].

2.1 Smart Grid Stability

There are three types of stability are considered for power systems: rotor angle stability, frequency stability, and voltage stability. Our research focuses on improving the rotor angle stability and frequency stability of the system in the face of large system disturbance. Therefore, let $\theta_i(t)$ denote the rotor phase angle of Generator i at time t and ω_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:

$$\left|\theta_i(t) - \theta_j(t)\right| \leq \gamma, \; for \; \forall t, \tag{1}$$

where the threshold γ is normally set as $5\pi/9$ in the realistic application as discussed in *[102];*

2. Exponential frequency synchronization:

$$\omega_i(t) \to 0, \; as \; t \to \infty. \tag{2}$$

2.2 Physical Dynamics and Interaction

According to the definition of Smart Grid Stability, the synchronous generators are the critical physical components. Therefore, modeling the physical dynamics of the synchronous generators and analyzing the interaction between them are necessary for maintaining smart grid stability. We describe the *physical* system by abstracting the information on the physical coupling between these critical components. We employ the well-known interconnected swing equations to describe rotor dynamics [78] of the Kron-reduced [15] power system as detailed by Dörfler and Bullo [34] to give the following dynamical representation for each agent:

$$M_i\dot{\omega}_i = -D_i\omega_i + P_{m,i} - |E_i|^2 G_{ii} - \sum_{j=1}^{N} P_{ij}\sin(\theta_i - \theta_j + \varphi_{ij}) \tag{3}$$

where $i \in \{1,2,...,N\}$ represents the generator index, θ_i denotes the rotor phase angle measured with respect to a rotating frame reference at frequency $f_0 = 60$ Hz, $\omega_i = \dot{\theta}_i$ is the normalized relative frequency, $M_i > 0$ and $D_i > 0$ represent the generator inertia and the damping parameters, respectively, and E_i, $P_{m,i}$ and G_{ii} are the internal voltage, mechanical power input and equivalent shunt conductance of Generator i, respectively. $P_{ij} = |E_i||E_j||Y_{ij}|$ and $\varphi_{ij} = \arctan(G_{ij}/B_{ij})$ where Y_{ij}, G_{ij} and B_{ij} are the Kron-reduced equivalent admittance, conductance and susceptance, respectively, between Generators i and j .

2.3 Hierarchical Cyber-Physical Integration Framework

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 phsyical systems work synergistically such that the bidirectional cyber information and power flows are efficiently used to enhance system resilience.

As stated in [103], 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 model the cyber-physical integration in the smart grid with a two-tier hierarchical multi-agent framework shown in Fig. 2.

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 6. 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.

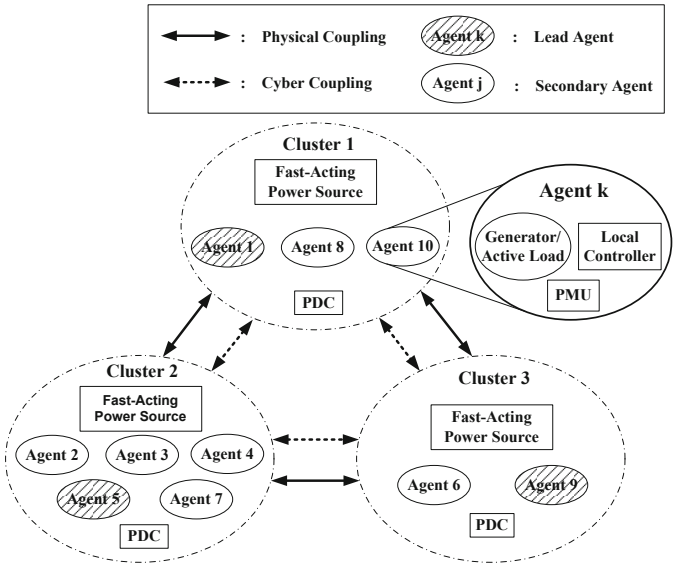


Fig. 2 Proposed two-tier hierarchical cyber-physical integrated multi-agent framework

We illustrate the implementation of the hierarchical control framework for the well-known New England 39-bus system in Fig. 3. 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). Since our focus is on 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. These storages in practice may include battery storage devices, flywheels, renewable energy sources, and other types of massive energy storage [7,49], and may be separate from each agent.

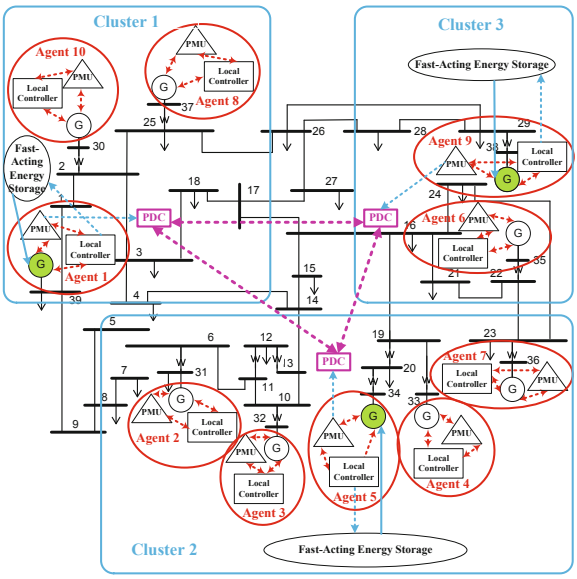


Fig. 3 Hierarchical cyber-physical control for New England 39-bus system

2.4 Cyber-Physical Interaction

We have introduced the concept of hierarchical cyber-physical integration framework for smart grids by modeling the system as a hierarchical multi-agent system. In this section, we continue to formulate the cyber-physical interaction between the multiple agents.

2.4.1 Dynamical Description of Cyber-Physical Interaction

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 α_i be a binary number defined as follows:

$$\alpha_i = \begin{cases} 1, \text{ if the } i\text{th agent is the lead agent;} \\ 0, \text{ otherwise,} \end{cases} \tag{4}$$

we can formulate the dynamics of our cyber-physical integrated framework as follows:

$$M_i\dot{\omega}_i = -D_i\omega_i + P_{m,i} - E_i^2 G_{ii} - \sum_{j=1, j\neq i}^{N} \underbrace{P_{ij}}_{\text{phys §}} \sin\left(\theta_i - \theta_j + \underbrace{\varphi_{ij}}_{\text{phys §}}\right) + \underbrace{\alpha_i u_i}_{\text{cyber §}}. \tag{5}$$

where u_i is the control signal for the ith agent computed from PMU data (θ_j, ω_j for $j \in \{1,2,...,N\}$). The control can be interpreted as power injection for $P_{u,i} > 0$ or absorption for $P_{u,i} < 0$ at the corresponding generator buses from the fast-acting external power sources. Thus, it represents a cyber-to-physical bridge whereby computation of u_i is converted to active power flow. Similarly, a physical-to-cyber bridge exists at the measurement devices in which physical phase angle and frequency are converted to PMU data. Thus, the dynamics of Eq. (5) represents both cyber and physical interactions. Physical inter-agent couplings (denoted phys §) are characterized by parameters P_{ij} and φ_{ij} and cyber couplings (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.

In order to reformulate the problem of cyber-physical control for maintaining transient stability as a task of flocking formation control, we intend to present the dynamics of each agent in our cyber-physical integrated system, which is originally formulated in Eq. (5), in the form of a double integrator model. Under these assumptions, computing derivatives of the both sides of Eq. (5), and reformulating gives:

$$\begin{cases} \dot{\theta} = \omega, \\ \mathbf{D}\dot{\omega} = -\mathbf{M}\ddot{\omega} - \mathbf{L}\omega + \alpha\dot{\mathbf{u}}. \end{cases} \tag{6}$$

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, $\alpha = \mathbf{diag}[\alpha_1, \ldots, \alpha_N]$, $\alpha_i = 1$ for $i \leq C$, and $\alpha_i = 0$ otherwise. $\theta = [\theta_1, \ldots, \theta_N]^T$, $\omega = [\omega_1, \ldots, \omega_N]^T$, $\mathbf{u} = [u_1, \ldots, u_N]^T$, $\mathbf{M} = \mathrm{diag}[M_1, \ldots, M_N]$, $\mathbf{D} = \mathrm{diag}[D_1, \ldots, D_N]$, and $\mathbf{L}$ is a $N \times N$ physical coupling matrix whose elements can be represented as:

$$l_{ij} = \begin{cases} \sum_{j=1, j\neq i}^{N} P_{ij} \cos(\theta_i - \theta_j + \varphi_{ij}), & \text{if } i = j; \\ -P_{ij} \cos(\theta_i - \theta_j + \varphi_{ij}), & \text{if } i \neq j, \end{cases} \tag{7}$$

2.4.2 Hierarchical Cyber-Physical Dynamics

In our hierarchical framework, the agents are grouped into the same cluster if they have high physical coherency. Since the term of Generator Coherency refers to the characteristics that the states of the coherent generators are close to each other [78], it is reasonable to 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 (θ_i, ω_i) of Secondary Agent i as "noisy" versions of those of Lead Agent k which is in its cluster and estimate (θ_i, ω_i) as follows:

$$\begin{cases} \widehat{\omega}_i = \omega_k + \triangle_i \\ \widehat{\theta}_i = \theta_k + \varepsilon_i^0 + \varsigma_i \end{cases} \tag{8}$$

where ε_i^0 denotes the phase angle difference between the ith and kth agents in the static (pre-fault) state, and $\triangle_i \sim \mathscr{U}(-a, a)$ and $\varsigma_i \sim \mathscr{U}(-b, b)$ are uniform random noises on $[-a, a]$ and $[-b, b]$, respectively, with $a \ll 1$ and $b \ll 1$.

By using Eq. (8), we are able to estimate the information of the physical coupling matrix $\mathbf{L}$ by only using the lead agents' states. To simplify, we partition $\mathbf{L}$ as follows:

$$\mathbf{L} = \begin{bmatrix} \mathbf{R}_{C\times C} & \mathbf{S}_{C\times(N-C)} \\ \mathbf{T}_{(N-C)\times C} & \mathbf{U}_{C\times C} \end{bmatrix}.$$

By using Eq. (8), we can approximate the matrix $\mathbf{S}$ with $\widehat{\mathbf{S}}$ whose element is shown as follows:

$$\widehat{\mathbf{S}}(j,k) = -P_{jk} \cos\left(\theta_j - \theta_k - \varepsilon_i^0 + \varphi_{jk}\right), \tag{9}$$

where the ith secondary agent belongs to the kth cluster. Using Eq. (9), we can approximate the matrix $\mathbf{R}$ by using $\widehat{\mathbf{R}}$ whose element is defined as follows:

$$\widehat{\mathbf{R}}(i,j) = \begin{cases} \mathbf{R}(i,j), & \text{if } i \neq j; \\ -\sum_{j=1, j\neq i}^{C} \mathbf{R}(i,j) - \sum_{j=C+1}^{N} \widehat{\mathbf{S}}(i,j), & \text{otherwise.} \end{cases} \tag{10}$$

Based on Eqs. (9), (10), (6), and (8), we achieve the hierarchical cyber-physical dynamics as follows:

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

$$\begin{cases} \dot{\theta}_l = \omega_l, \\ \mathbf{D}_l \dot{\omega}_l = -\mathbf{M}_l \ddot{\omega}_l - \left(\widehat{\mathbf{R}} + \widehat{\mathbf{S}}\Psi\right) \omega_l + \dot{u}_l - \widehat{\mathbf{S}}\triangle, \end{cases} \tag{11}$$

where the subscript, $\omega_l = [\omega_1, \ldots, \omega_C]^T$, $\theta_l = [\theta_1, \ldots, \theta_C]^T$ $\mathbf{D}_l = \text{diag}[D_1, \ldots, D_C]$, $\mathbf{M}_l = \text{diag}[M_1, \ldots, M_C]$, $\mathbf{u}_l = [u_1, \ldots, u_C]^T$, $\triangle = [\triangle_{C+1}, \ldots, \triangle_N]^T$,

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

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

$$\begin{cases} \dot{\theta}_s = \omega_s, \\ \mathbf{D}_s \dot{\omega}_s = -\mathbf{L}_s \omega_s - \mathbf{M}_s \ddot{\omega}_s, \end{cases} \tag{12}$$

where $\mathbf{L}_s$ denotes the physical coupling matrix for secondary agents, $\mathbf{M}_s = \text{diag}[M_{C+1}, \ldots, M_N]$, $\theta_s = [\theta_{C+1}, \cdots, \theta_N]^T$, and $\omega_s = [\omega_{C+1}, \cdots, \omega_N]^T$.

3 Hierarchical Control Protocol Design by Analogy to Flocking

Based on the dynamical modeling of the hierarchical cyber-physical integration framework introduced above, we design the control protocol to maintain the smart grid stability in the emergent situation by leveraging the flocking theory.

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 [99], 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 [95] provided a framework for design and analysis of scalable distributed flocking algorithms using a double integrator model:

$$\begin{cases} \dot{\mathbf{q}} = \mathbf{p} \\ \dot{\mathbf{p}} = \mathbf{u}, \end{cases} \tag{13}$$

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

To achieve the objectives of flocking, the control signal $\mathbf{u}$ is comprised of three terms:

$$\mathbf{u} = -\nabla V(\mathbf{q}) - \mathbf{L} \cdot \mathbf{p} + F(\mathbf{p}, \mathbf{q}, \mathbf{p}_r, \mathbf{q}_r). \tag{14}$$

The first term is the gradient of a potential energy function $V(\mathbf{q})$ which characterizes system objectives and constraints. The second term represents a velocity consensus protocol where $\mathbf{L}$ 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 $(\mathbf{p}_r, \mathbf{q}_r)$.

The stability of the control protocol described in Eq. (14) has been analyzed in [95] to provide the following sufficient conditions for stability: (1) $V(\mathbf{q})$ is a nonnegative continuously differentiable potential energy function that achieves the global minimum at a desired formation; (2) $\mathbf{L}$ is a standard Laplacian matrix, which is positive semidefinite and has a zero row sum [92]; (3) $F(\mathbf{p}, \mathbf{q}, \mathbf{p}_r, \mathbf{q}_r)$ is a linear combination of $(\mathbf{p} - \mathbf{p}_r)$ and $(\mathbf{q} - \mathbf{q}_r)$.

3.2 Design by Analogy to Flocking

Let the state of each agent be given by $(\theta_i(t), \omega_i(t))$, which is the associated generator's state. Given the self-regulation goals of the transient stability problem, we consider cyber-control between agents using *deviations* of their phase angle $\theta_i(t) - \theta_j(t)$ and frequency $\omega_i(t) - \omega_j(t)$. In doing this, we are able to recognize the analogies between the transient stability problem and that of flocking. The problem of transient stabilization becomes equivalent to that of designing the collective cyber-physical dynamics of smart grid agents to be analogous to a stable flock of birds. This is achieved through the appropriate computation of cyber dynamics u_i using PMU data, which is then converted to energy injection/absorption $P_{u,i}$ at Generator Bus i.

We design u_i as follows:

$$u_i = -B_i \omega_i + h_i(\theta, \omega), \tag{15}$$

where B_i is a cyber parameter which satisfies that $B_i \geq (100 \times D_i)$ and $h_i(\cdot) : \mathbb{R}^N \times \mathbb{R}^N \to \mathbb{R}$ is a function of the vector $\theta = \{\theta_i | i \in \mathscr{I}_C\}$ and the vector $\omega = \{\omega_i | i \in \mathscr{I}_C\}$, and $\mathscr{I}_C$ represents the index set of the lead agents. We can rewrite the second line of Eq. (11) as follows:

$$(\mathbf{D}_l + \mathbf{B})\,\dot{\omega}_l = -\mathbf{M}_l \ddot{\omega}_l - \left(\widehat{\mathbf{R}} + \widehat{\mathbf{S}}\Psi\right)\omega_l + \mathbf{h} - \widehat{\mathbf{S}}\triangle, \tag{16}$$

where $\mathbf{B}$ is a pre-designed $C \times C$ cyber coupling diagonal matrix with diagonal element B_i and $\mathbf{h}$ is a C-dimensional cyber control column vector with: ith element is as follows:

$$h_i = \begin{cases} \frac{d}{dt} h_i(\theta, \omega), & \text{if } i = 1, \ldots, C; \\ 0, & \text{otherwise,} \end{cases} \tag{17}$$

In practice, for the ith synchronized generator, the ratio between the inertia M_i and the damping parameter D_i satisfies $M_i/D_i \in \mathscr{O}(10)$ [102]. We therefore find that the associated perturbation parameter for Lead Agent i is $\varepsilon_i = M_i/(D_i + B_i) \in \mathscr{O}(0.1)$ representing an *overdamped* system, which enables the application of singular perturbation techniques to in Eq. (16) to study the dynamics of the lead agents over a longer time scale. Specifically, applying singular perturbation analysis and letting $\mathscr{M} = \mathbf{D}_l + \mathbf{B}$ [65] gives:

$$\begin{cases} \dot{\theta}_l = \omega_l, \\ \mathscr{M}\dot{\omega}_l = -\left(\widehat{\mathbf{R}} + \widehat{\mathbf{S}}\Psi\right)\omega_l + \mathbf{h} - \widehat{\mathbf{S}}\triangle, \end{cases} \tag{18}$$

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

Since the nonlinear dynamical system of Eq. (18) is feedback linearizable, we can define a new control vector $\widetilde{\mathbf{u}}$ and rewrite the equivalent reduced order model as:

$$\begin{cases} \dot{\theta}_l = \omega_l, \\ \mathscr{M}\dot{\omega}_l = \widetilde{\mathbf{u}} - \widehat{\mathbf{S}}\Delta. \end{cases} \tag{19}$$

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

$$\dot{\mathbf{u}} = \widetilde{\mathbf{u}} + \left(\widehat{\mathbf{R}} + \widehat{\mathbf{S}}\Psi\right)\omega_l - \mathbf{B}\dot{\omega}_l. \tag{20}$$

Equation (19) represents a double integrator system analogous to Eq. (13) known to model the standard dynamics of flockings. By setting $\widetilde{\mathbf{u}}$ to the following form we thus ensure flocking formation and hence transient stability of the power network:

$$\widetilde{\mathbf{u}} = \underbrace{-\nabla V(\theta_l)}_{\text{phase cohesiveness}} - \underbrace{\widetilde{\mathbf{L}}\omega_l + F(\omega_l, \omega_r)}_{\text{frequency synchronization}}, \tag{21}$$

where $V(\theta_l)$ represents the potential energy function to guarantee that the phase angle differences between pairs of lead agents are bounded, $\nabla V(\theta_l)$ is its associated gradient with respect to θ_l, $\widetilde{\mathbf{L}}$ is the effective Laplacian matrix that ensures frequency consensus (i.e., lead 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 ω_r; typically relative frequency is normalized such that $\omega_r = 0$.

3.2.1 Potential Energy Function

Based on the sufficient condition of Eq. (1), we consider the following potential energy for our control scheme:

$$V(\theta_l) = \frac{1}{2}\sum_{i=1}^{C}\sum_{j=1,j\neq i}^{C}\chi\left(\theta_i - \theta_j\right), \tag{22}$$

where $\chi(\cdot)$ is a pairwise attractive potential defined as:

$$\chi(z) = \begin{cases} 0, & \text{if } |z| \leq \frac{5\pi}{9}; \\ c_1\left(z^2 - \frac{25\pi^2}{81}\right)^2, & \text{otherwise,} \end{cases} \tag{23}$$

where c_1 is a parameter to control the penalty level induced. It can be shown that $\chi(\cdot)$ is continuously differentiable and thus the gradient $\boldsymbol{\Phi}$ can be represented as follows:

$$\begin{aligned} \boldsymbol{\Phi}(i) &= \sum_{j=1,j\neq i}^{C}\phi\left(\theta_i - \theta_j\right), \\ \phi(z) &= \begin{cases} 0, & \text{if } |z| \leq \frac{5\pi}{9}; \\ 4c_1 z\left(z^2 - \frac{25\pi^2}{81}\right), & \text{otherwise.} \end{cases} \end{aligned} \tag{24}$$

3.2.2 Effective Laplacian

As illustrated in [117], we deduce that a sufficient condition to ensure $\widetilde{\mathbf{L}}$ is PSD is $\widetilde{l}_{ij} < 0$ where $i \neq j$. Furthermore, 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 $\widetilde{\mathbf{L}}$ to be symmetric. Therefore, in our framework, we design the ijth element of the effective Laplacian matrix $\widetilde{\mathbf{L}}$ as follows:

$$\widetilde{l}_{ij} = \begin{cases} c_2, & \text{if } i = j; \\ \frac{c_2}{C-1}, & \text{otherwise.} \end{cases} \tag{25}$$

3.2.3 Linear Navigation Feedback

To reduce complexity, we assign the following linear navigation feedback term: $F(\omega_l, \omega_r) = c_3\omega_l$, where c_3 is a cyber control parameter.

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

$$\widetilde{\mathbf{u}} = -\boldsymbol{\Phi} - \widetilde{\mathbf{L}}\omega_l - c_3\omega_l, \tag{26}$$

Using Eqs. (20) and (26), we obtain the following result:

$$\dot{\mathbf{u}} = -\boldsymbol{\Phi} + \left(\widehat{\mathbf{R}} + \widehat{\mathbf{S}}\boldsymbol{\Psi}\right)\omega_l - \widetilde{\mathbf{L}}\omega_l - c_3\omega_l - \mathbf{B}\dot{\omega}_l. \tag{27}$$

By integrating both sides of Eq. (27), we can formulate $\mathbf{u}$, which represents the power transmission $\mathbf{P}_u$ between the fast-reacting power source and the synchronized

generators, as:

$$\mathbf{u} = -\Gamma + \int_{t_0}^{t} \left(\widehat{\mathbf{R}} + \widehat{\mathbf{S}}\Psi\right) \omega_l d\tau - \widetilde{\mathbf{L}}\theta_l - c_3\theta_l - \mathbf{B}\omega_l, \tag{28}$$

where θ_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:

$$\Gamma(i) = \sum_{j=1, j\neq i}^{C} \left[\int_{t_0}^{t} \phi\left(\theta_i - \theta_j\right)\right] d\tau. \tag{29}$$

Let the C-dimension column vector η denote $\int_{t_0}^{t} \left(\widehat{\mathbf{R}} + \widehat{\mathbf{S}}\Psi\right) \omega_l d\tau$. Since $\widehat{\mathbf{R}}$, $\widehat{\mathbf{S}}$, and θ are time-varying, and the information of them is available, using Eqs. (7) and (9) we obtain:

$$\begin{aligned}\eta(i) &= \sum_{j=1, j\neq i}^{C} \int_{t_0}^{t} \left[P_{ij}\cos\left(\theta_{ij} + \varphi_{ij}\right) + \sum_{k\in\mathscr{I}_j} P_{ik}\cos\left(\theta_{ij} - \varepsilon_k^0 + \varphi_{ik}\right)\right] \omega_{ij} d\tau, \\ &= \sum_{j=1, j\neq i}^{C} P_{ij}\sin\left(\theta_{ij} + \varphi_{ij}\right) + \sum_{j=1, j\neq i}^{C} \sum_{k\in\mathscr{I}_j} P_{ik}\sin\left(\theta_{ij} - \varepsilon_k^0 + \varphi_{ik}\right) - \eta_i^0, \end{aligned} \tag{30}$$

where $\mathscr{I}_j$ denotes the index set of the secondary agents belonging to the jth cluster, $\omega_{ij} = \omega_i - \omega_j$, $\theta_{ij} = \theta_i - \theta_j$, and

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

3.3 Hierarchical Control Protocol Stability Analysis

We define the following Lyapunov function H:

$$H = \frac{1}{2}\omega_l^T \mathbf{M}\omega_l + \mathbf{V} \tag{31}$$

for which $H(\mathbf{0}, \mathbf{0}) = 0$ and $H(\theta, \omega_l) > 0$ for $\forall(\theta, \omega_l) \neq (\mathbf{0}, \mathbf{0})$. Calculating the derivative of H along the dynamics derived in Eqs. (19) and (26) we obtain:

$$\dot{H} = \omega_l^T \mathbf{M}\dot{\omega}_l + \omega_l^T \nabla V = -\omega_l^T \left(\widetilde{\mathbf{L}} + c_3\mathbf{I}\right) \omega_l - \omega_l^T \widehat{\mathbf{S}}\Delta. \tag{32}$$

Based on our proposed framework, $\widetilde{\mathbf{L}}$ is the effective Laplacian matrix which is PSD and $c_3 > 0$. Therefore, $\left(\widetilde{\mathbf{L}} + c_3\mathbf{I}\right)$ is a Positive Definite (PD) matrix. Using the property of PD matrices, we deduce $\omega_l^T \left(\widetilde{\mathbf{L}} + c_3\mathbf{I}\right) \omega_l > 0$.

Since information on ω_l and $\widehat{\mathbf{S}}$ is available and $\widetilde{\mathbf{L}}$ and c_3 are designable, using Lyapunov redesign, we obtain:

$$\dot{H} \leq -\lambda_m \|\omega_l\|^2 + \rho \|\omega_l\| \|\widehat{\mathbf{S}}\| = -\|\omega_l\| \left(\lambda_m \|\omega_l\| - \rho \|\widehat{\mathbf{S}}\|\right) \tag{33}$$

where λ_m is the smallest eigenvalue of $\left(\widetilde{\mathbf{L}} + c_3 \mathbf{I}\right)$.

Since $\widetilde{\mathbf{L}}$ is a Laplacian with minimum eigenvalue 0, $\lambda_m = c_3$. Therefore, $\dot{H} < 0$ is guaranteed when:

$$\|\omega_l\| \geq \frac{\rho \|\widehat{\mathbf{S}}\|}{c_3}. \tag{34}$$

The high physical coherency between intra-cluster agents ensures that ρ 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:

$$c_3 \geq \frac{\rho \|\widehat{\mathbf{S}}\|}{0.02}. \tag{35}$$

Based on Eqs. (34) and (35), 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 transient stability given the existence of an accurate and efficient coherent cluster identification algorithm.

4 Timely Dynamic Agent Coherency Identification

In order to efficiently implement the hierarchical control framework illustrated above, it is necessary to rapidly identify the agent coherency with high accuracy. In this section, we propose a timely dynamic agent coherency identification scheme which requires very short observation window. Our scheme transforms the data of agents' state from the observation space to an information space whereby the agents' frequencies and phases characterize the movement and dynamics of boids within multiple flocks with different features. Boid i carries three-dimensional information describing the ith agent's status at time $t = k$ as:

$$\begin{cases} \mathscr{I}_i^1(k) = \theta_i(k) \\ \mathscr{I}_i^2(k) = \omega_i(k) \\ \mathscr{I}_i^3(k) = \delta_i(k) \end{cases}, \tag{36}$$

where $\mathscr{I}_i(k) = [\mathscr{I}_i^1(k)\ \mathscr{I}_i^2(k)\ \mathscr{I}_i^3(k)]^T$, $\theta_i(k)$ and $\omega_i(k)$ are the phase angle and the normalized frequency, respectively, of the ith generator at the time step $t = k$ that are obtained directly from PMU information, and $\delta_i(k)$ is the acceleration of the ith generator at the time step $t = k$ estimated from the current and historical values of $\omega_i(k)$.

The state of Boid i is described as follows:

$$\mathscr{S}_i(k) = [\mathbf{p}_i(k), \mathbf{v}_i(k)]^T, \tag{37}$$

where $\mathbf{p}_i(k), \mathbf{v}_i(k) \in \mathbb{R}^{2\times 1}$ denote the boid's position and the velocity, respectively. Two boids are considered to be neighbors at time step $t = k$ if the distance between them is less than the predetermined threshold d_c. Therefore, we define the set of neighbors for the ith boid as follows: $\mathscr{N}_i(k) = \{\forall j \big| \|\mathbf{p}_i(k) - \mathbf{p}_j(k)\| < d_c\}$.

We compute the *informational* (feature) *similarity* between neighboring Boids i and j as follows. For $j \in \mathscr{N}_i(k)$,

$$\zeta_{ij}(k) = \Big| \sum_{n=1}^{3} \alpha_n \times \big(\mathscr{I}_i^n(k) - \mathscr{I}_j^n(k)\big) \Big|, \tag{38}$$

where $\{\alpha_n\}$ is a scalar weight determining the impact of specific information on boid interaction. Given a threshold value $\zeta_{th}(k)$, if $\zeta_{ij}(k) \le \zeta_{th}(k)$ they are assumed to be in the same flock and hence are called *flockmates*. Otherwise, they are assumed to be in different flocks.

As illustrated in detail in [115], we model the dynamics of Boid i based on their feature similarity and flocking rules as:

$$\begin{cases} \mathbf{v}_i(k+1) = \mathbf{v}_i(k) + \Delta t \sum_{l=1}^{3} w_l \mathbf{g}_{i,l}(k), \\ \mathbf{p}_i(k+1) = \mathbf{p}_i(k) + \Delta t \mathbf{v}_i(k), \end{cases} \tag{39}$$

where $\mathbf{g}_{i,1}, \mathbf{g}_{i,2}, \mathbf{g}_{i,3}$ represent the accelerations calculated based on the flocking rules *flock centering*, *velocity matching*, and *obstacle avoidance*, respectively, w_l denotes the weight representing the impact of the component $\mathbf{g}_{i,l}$, and Δt is the algorithm time step for coherence identification.

Based on dynamic model in Eq. (39), we can plot the boids' trajectories in the information space and achieve the multiple flocks constituted by the boids, which corresponds to the clusters constituted by the agents having high physical coherency in the observation space.

5 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. 4.

Threat Model: Let H_k be the number of agents in the kth 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

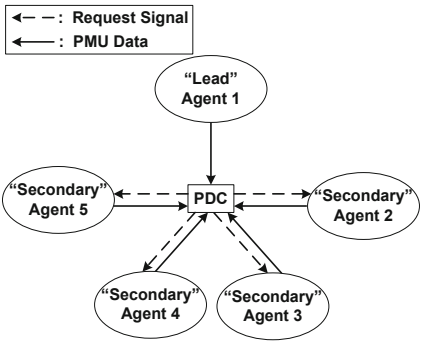


Fig. 4 Communication between PDC and agents locally within each cluaster

readings or equivalently replacing true values with fabricated quantities over a verification *period.*

As described in Eq. (8), 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 1. Since our proposed flocking-based control protocol is robust to the biases on the measurement of the lead agents' frequency [96], 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 ℓ most recent bias samples $\{\xi_i | i \in \mathscr{I}\}$ for possible future estimation use. Otherwise, it estimates the true value using the proposed cyber-physical estimation scheme of Table 2.

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. (11) is guaranteed analytically [116], 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

Table 1 Proposed Cyber-Physical Verification Scheme

Let the lead agent PMU reading be θ^c. Let the secondary agents be represented with indices from the set $i \in \mathscr{I}$ and their readings be denoted θ_i. Let $\Delta\theta_i$ be the phase angle difference between θ_i and θ^c at static state (i.e., pre-fault).
We assign $H_k = |\mathscr{I}| + 1$.
1. Initialize $Count = 0$ and set the threshold τ_p.
2. For each $i \in \mathscr{I}$
   $\xi_i = \theta_i - \Delta\theta_i - \theta^c$,
   If $\xi_i \leq \tau_p$
   $Count = Count + 1$,
   End
   End
3. If $Count < \left\lfloor \frac{1}{2} H_i \right\rfloor + 1$
   The PDC reports the lead agent's PMU as being attacked,
   Else
   The PDC reports the lead agent's PMU as valid,
   End

Table 2 Proposed Cyber-Physical Estimation Scheme

Let the secondary agents be represented with indices from the set $i \in \mathscr{I}$. Let $\xi_i \in \mathbb{R}^\ell$ be a vector containing the ℓ most recent sample values of ξ_i in chronological order. Let $a(n)$ be an ℓ-point Hamming window.
1. For each $i \in \mathscr{I}$
   Secondary agent estimates lead agent phase angle using Eq. (8).
   Secondary agent reports the estimation result $\widehat{\theta}_i^c$ to the PDC.
   End
2. The PDC evaluates estimation accuracy for $i \in \mathscr{I}$ by computing:

$$\widehat{\sigma}_i = \sqrt{\frac{\sum_{n=1}^{\ell} a(n-1)\xi_i(n)^2}{\sum_{n=1}^{\ell} a(n-1)}}. \tag{40}$$

3. The PDC forms $\widehat{\theta}_l$ consisting of elements $\widehat{\theta}_i^c, i \in \mathscr{I}$ ordered to reflect monotonically increasing values in $\widehat{\sigma}_i$.
4. The PDC estimates θ^c from a median-like value from the elements of $\widehat{\theta}_l$ to avoid extreme biases:

$$\widehat{\theta}^c = \begin{cases} \widehat{\theta}_l\left(\frac{1}{2}H_k\right), & \text{if } H_k \text{ is even;} \\ \frac{1}{2}\left[\widehat{\theta}_l\left(\frac{1}{2}(H_k-1)\right) + \widehat{\theta}_l\left(\frac{1}{2}(H_k-1)+1\right)\right], & \text{otherwise} \end{cases}$$

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.

6 Simulations and Performance Assessment

We demonstrate the performance of our flocking-based two-tier hierarchical control framework with dynamics in Eqs. (11) and (12) collectively also described by Eq. (5) in achieving smart grid stability for two case studies on the New England 39 Bus system as shown in Fig. 5 and detailed in [13] consisting of $C = 10$ generators. MATLAB/Simulink is employed for simulations. 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. (28) are set to $c_1 = 5$, $c_2 = \frac{1}{10}$ and $c_3 = 3$, and the PMU sampling rate is 50 Hz. The power transmission limit for the fast-acting grid is set to $\mu = P_{u,i}/P_{r,i} \leq 1$ where $P_{r,i}$ is the rated power.

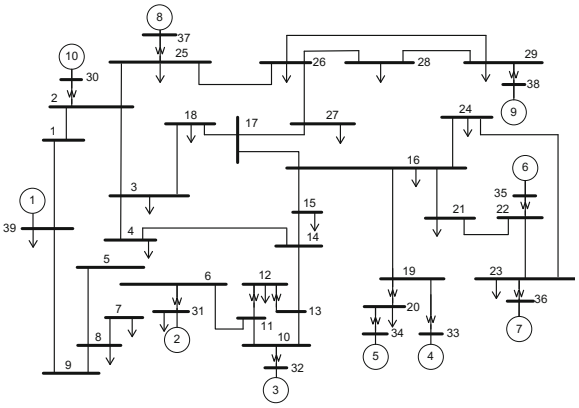


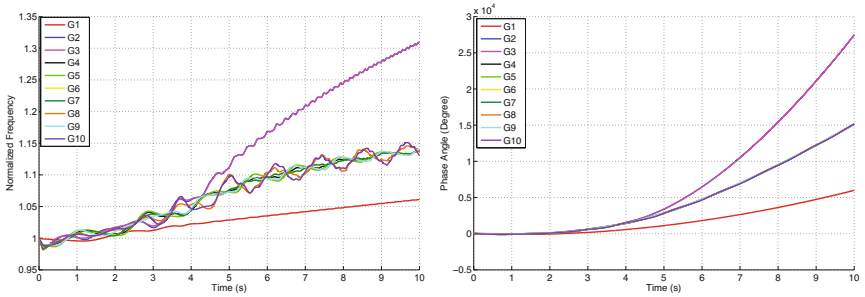
Fig. 5 New England 39-bus power system

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.

6.1 Ideal Environment

6.1.1 Case I

The system disturbance consists of a 3-phase short circuit in the middle of Line $14-15$ of Fig. 5 which occurs at time $t=0$ s. The Line $14-15$ is removed at $t=0.1$ s. Fig. 6 shows the normalized rotor frequencies and phase angles over a period of 10 s when no control is applied corresponding to Eq. (6) for $\alpha_i=0$ for all i. Instability is clearly evident in all plots.

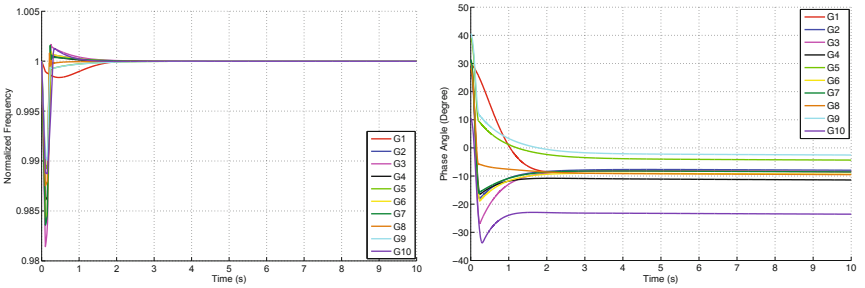


(a) (b)

Fig. 6 (a) Normalized rotor frequencies and (b) phase angles without cyber control

Fig. 7 (note: scale differs from Fig. 6) demonstrates performance for *non-hierarchical* cyber-physical control activated at time $t=0.15$ s, in which the PMU of each agent is activated and cyber control works at each agent. This *non-hierarchical* framework can be mathematically described by using Eq. (6) which $\alpha_i=0$ for all Agent i. The EES power absorbtion/injection to each generator bus, determined by the control signal $\mathbf{u}$, is shown in Fig. 8. Even though the clipping of the control signal occurs due to the capacity limit previously discussed, smart grid stability is still achieved.

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 boid trajectories introduced by the flocking analogy used in our agent coherency identification scheme is presented in Fig. 9(a) for a very brief observation period of $t=0.05$ s; as described in Eq. (36), each boid carries the information describing the associated agent's status. The neighboring boids interact with each other based on the informational similarity which is defined in Eq. (38) and their dynamics are modeled in Eq. (39). From Fig. 9(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



(a) (b)

Fig. 7 (a) Normalized rotor frequencies and (b) Phase angles with the non-hierarchical control

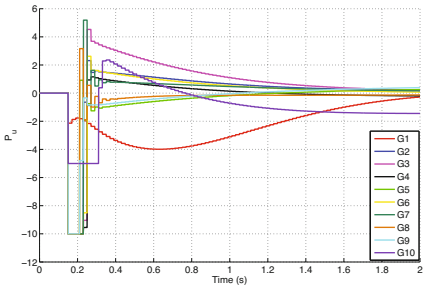
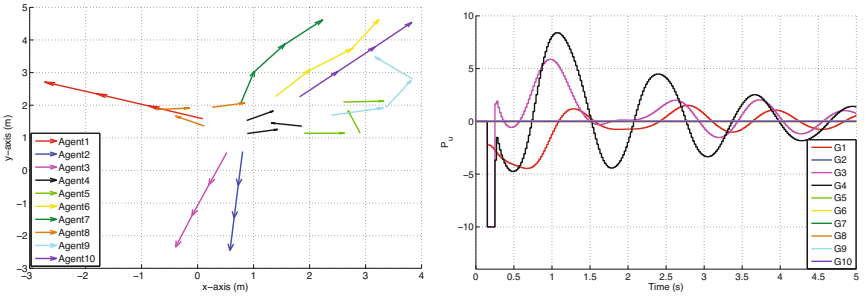


Fig. 8 Power transfer P_u by fast acting energy storage at generator buses in the presence of non-hierarchical control for Case Study I

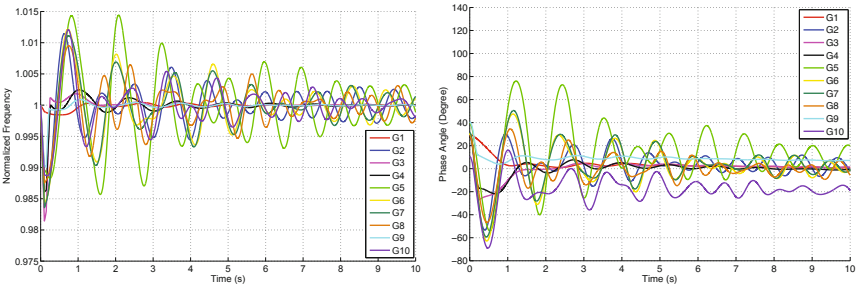
clusters are *Agent* 1, *Agent* 3 and *Agent* 4, which have larger inertia compared with other agents belonging to the same cluster. 3) After determining the hierarchical framework, at time $t = 0.15$ s, our proposed two-tier hierarchical cyber-physical control framework is activated which controls the 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. (28) and is plotted in Fig. 9(b). As shown in Fig. 9(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 nonhierarchy, 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 10 presents the generator frequencies and phase angles by using our proposed two-tier hierarchical cyber-physical control framework. In contrast to Fig. 6 in which there is no control, smart grid stabilization is evident. In contrast to the non-



(a) (b)

Fig. 9 (a) The trajectories of the boids 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



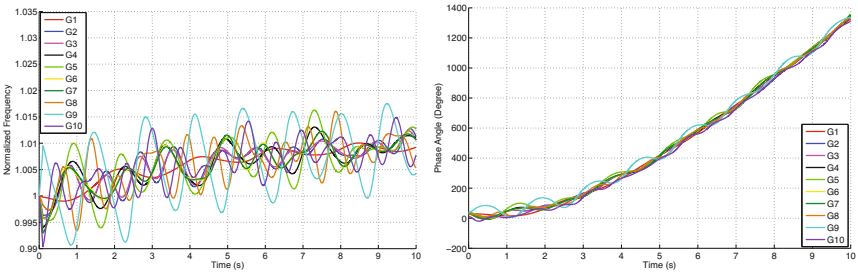
(a) (b)

Fig. 10 (a) Normalized rotor frequencies and (b) phase angles with hierarchical control

hierarchical case shown in Fig. 7, there is more high frequency oscillatory behavior due to the nature of the activated EES power outputs. From Fig. 10, 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.

6.1.2 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. 5. The Line $17-27$ is removed at $t = 0.1$ s. Figure 11 shows the normalized rotor frequencies and phase angles over a period of 10 s when no control is applied. Based on Fig. 11, we assess smart grid stability of the system by calculating the power angle-based stability margin ξ [78], and achieve $\xi_1 = 57.1$ which implies that the system smart grid security is low and very sensitive to perturbation. Parameter $\xi = \frac{360-\delta_{max}}{360+\delta_{max}} \times 100$ where δ_{max} is the maximum angle separation of any two generators at the same time in the post-fault response, and $-100 < \xi < 100$.



(a) (b)

Fig. 11 (a) Normalized rotor frequencies and (b) phase angles without cyber control

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 boid trajectories introduced by the flocking analogy used in our agent coherency identification scheme is presented in Fig. 12 for a very brief observation period of $t = 0.05$ s. From Fig. 12, we determine that our two-tier hierarchical framework consists of the clusters $\{Agent_1, Agent_{10}\}$, $\{Agent_2, \ldots, Agent_8\}$, and $\{Agent_9\}$, and the lead agents for these three clusters are *Agent* 1, *Agent* 4 and *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.

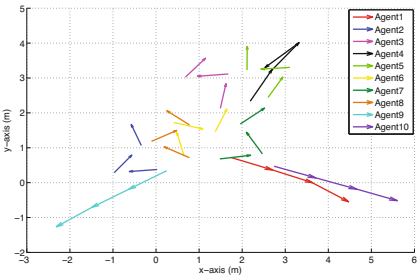
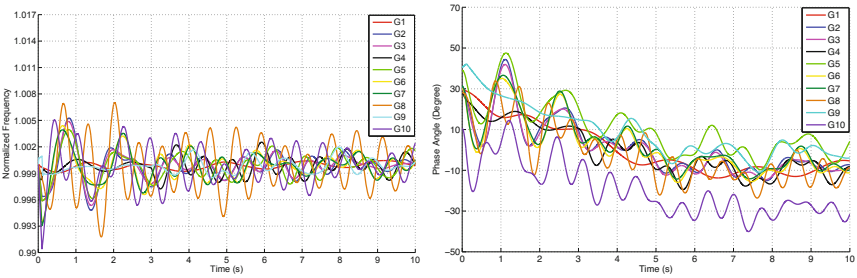


Fig. 12 The trajectories of the boids for Case Study II

Figure 13 evaluate the performance of normalized rotor frequencies and phase angles by using our proposed hierarchical control framework and Figure. 14 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.



(a) (b)

Fig. 13 (a) Normalized rotor frequencies and (b) phase angles with hierarchical framework

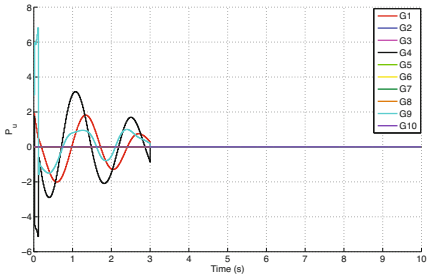


Fig. 14 Power transfer P_u

6.2 *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./Δt, 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 15 evaluates, given different values of ρ_1, the minimum value of ρ_2 required for maintaining smart grid stability by using hierarchical and non-hierarchical frameworks in Case I. Figure 15 also evaluates the minimum value of ρ_2 required for improving ξ equivalent to ensuring $\xi > 57.1$ versus different values of ρ_1 by using hierarchical and non-hierarchical frameworks in Case II. From Fig. 15, 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 15 also indicates that in Case II, the hierarchical and non-hierarchical framework desire the same physical requirement for energy storage.

In order to analyze the performance of our proposed control framework under the two constraints in more detail, Fig. 16 evaluates the power angle-based margin ξ achieved by implementing our control framework when $\rho_1 \in [1,5]$ and $\rho_2 \in [0.1,0.5]$. From Fig. 16(a), it is clear that in Case I the proposed hierarchi-

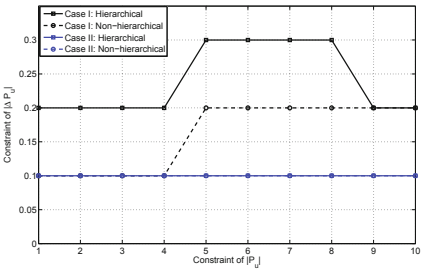


Fig. 15 Performance evaluation of Cases I and II by considering physical constraints of fast-acting energy storage

cal 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. 16(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. 16 are consistent with the conclusion got from Fig. 15. 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.

Figure. 17 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 $\rho_2 = 0.3$ in Case I, and Fig. 18 shows the generators' normalized rotor

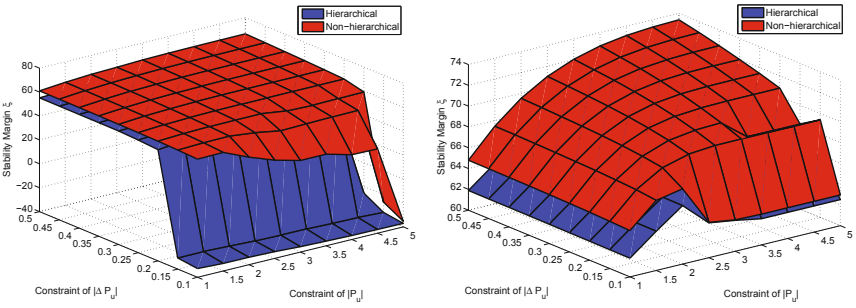


Fig. 16 The stability margin achieved under the practical constraints in (a) Case Study I and (b) Case Study II

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.

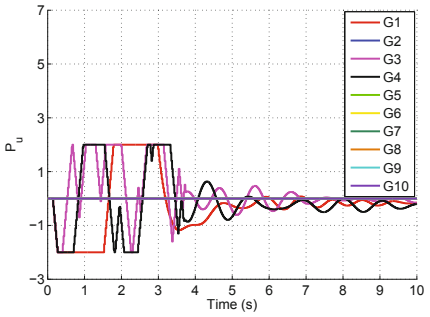
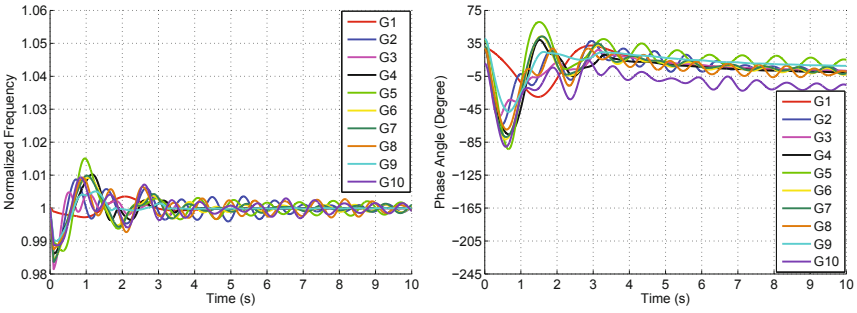


Fig. 17 Power transfer P_u by fast acting energy storage at generator buses



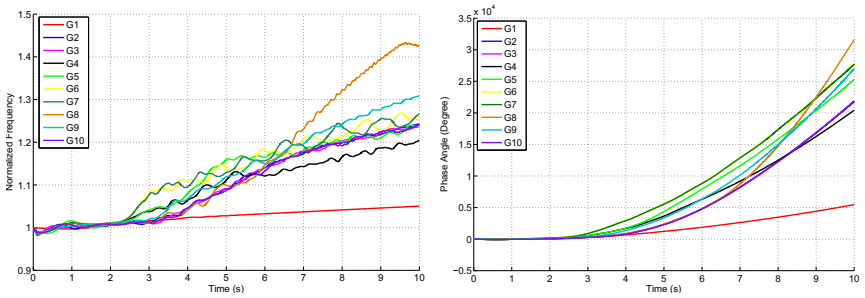
(a) (b)

Fig. 18 (a) Normalized rotor frequencies and (b) phase angles versus time

6.3 Environment with PMU Data Corruption

In our 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 $\tau_p = 35^\circ$. Figures 19 and 20 show the normalized frequencies, rotor phase angles, and P_u in the presence of information corruption on Agent 4, 6 and 7 when no witness-based cyber protection is applied. The compromised PMUs of Agent 4, 6 and 7 collude and report the same biased readings (bias = -257.8°) starting at $t = 0.5$ s for duration 2.5 s, 3 s, and 2 s, respectively. From Figs. 19 and 20, 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.



(a) (b)

Fig. 19 (a) The normalized frequencies and (b) the rotor phase angles versus time without proposed cyber-physical security protocol in presence of random attack.

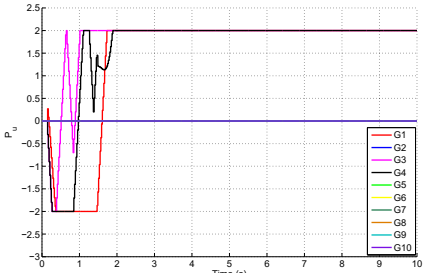
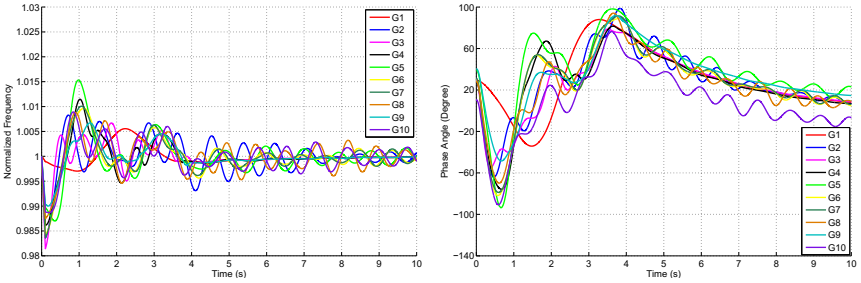


Fig. 20 P_u versus time without proposed cyber-physical security protocol in presence of random attack

Figures 21 and 22 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 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.

These simulation results illustrate that our proposed cyber-physical verification and estimation schemes can efficiently identify and correct the corrupted lead agents' PMUs' readings 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 5 is satisfied.



(a) (b)

Fig. 21 (a) The normalized frequencies and (b) the rotor phase angles versus time with proposed cyber-physical security protocol in presence of random attack

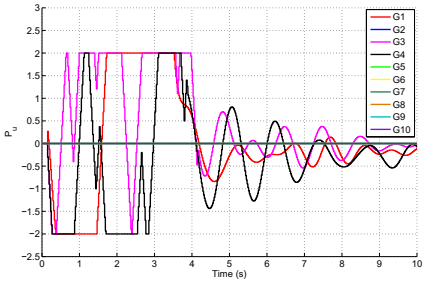


Fig. 22 P_u versus time with proposed cyber-physical security protocol in presence of random attack

7 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 chapter, we present a biologically-inspired cyber-physical multi-agent distributed control framework for maintaining smart grid stability under various forms of physical and cyber attacks. Through this multi-agent control framework, we demonstrate real-time cyber-physical integrated 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 hierarchical 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 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.

References

1. NERC CIP standards, http://www.nerc.com
2. Reliability considerations from the integration of smart grid. North American Electric Reliability Corporation (2010)
3. Roadmap to achieve energy delivery system cyber security. Energy Sector Control Systems Working Group (ESCSWG) (2011)
4. Intelligrid program: 2012 annual review. Electric Power Research Institute (EPRI) (2013)
5. Smart grids and renewables: A guide for effective deployment. International Renewable Energy Agency (IRENA) (2013)
6. How much electricity does an american home use? (2014), http://www.eia.gov/tools/faqs/faq.cfm?id=97&t=3
7. Adeodu, O., Chmielewski, D.: Design of massive energy storage systems within electric transmission networks. In: 2013 AIChE Annual Meeting, San Francisco, CA (2013)
8. Almond, S.J., Baird, S., Flynn, B.F., Hawkins, D.J., Mackrell, A.J.: Integrated protection and control communications outwith the substation: Cyber security challenges. In: Proc. IET 9th International Conference on Developments in Power System Protection, pp. 698–701 (2008)
9. Amin, S., Cárdenas, A.A., Sastry, S.S.: Safe and secure networked control systems under denial-of-service attacks. In: Majumdar, R., Tabuada, P. (eds.) HSCC 2009. LNCS, vol. 5469, pp. 31–45. Springer, Heidelberg (2009)
10. Amin, S.M.: Energy infrastructure defense systems. Proceedings of the IEEE 93(5), 861–875 (2005)
11. Amina, M., Stringer, J.: The electric power grid: Today and tomorrow. MRS Bulletin 33, 399–407 (2008)
12. Ananad, M., Cronin, E., Sherr, M., Blaze, M., Ives, Z., Lee, I.: Security challenges in next generation cyber physical systems. In: Proc. Beyond SCADA: Cyber Physical Systems Meeting (HCSS-NEC4CPS), Pittsburgh, Pennsylvania (2006)
13. Athay, T., Podmore, R., Virmani, S.: A practical method for the direct analysis of transient stability. IEEE Transactions on Power Apparatus and Systems PAS-98, 573–587 (1979)
14. Bakken, D.E., Hauser, C.H., Gjermundrod, H., Bose, A.: Toward more flexible and robust data delivery for monitoring and control of the electric power grid. Technical Report EECS-GS-009, Washington State University, Pullman, Washington (2007)
15. Bergen, A.R., Vittal, V.: Power Systems Analysis. Prentice Hall (1999)

16. Bobba, R., Khurana, H., AlTurki, M., Ashraf, F.: PBES: A policy based encryption system with application to date sharing in the power grid. In: Proc. ACM Sympoisum of Information, Computer and Communications Security, ASIACCS 2009, pp. 262–275 (2009)
17. Bobba, R., Rogers, K.M., Wang, Q., Khurana, H., Nahrstedt, K., Overbye, T.J.: Detecting false data injection attacks on DC state estimation. In: Proc. First Workshop on Secure Control Systems, Stockholm, Sweden (2010)
18. Byres, E., Chauvin, B., Hoffman, J., Kube, N.: The special needs of SCADA/PCN firewalls: Architectures and test results. In: Proc. 10th IEEE Conference on Emerging Technologies and Factor Automation, vol. 2, pp. 877–884 (2005)
19. C1 Working Group Members of Power System Relaying Committee: Cyber security issues for protective relays. In: Proc. IEEE Power Engineering Society General Meeting, pp. 1–8 (2007)
20. Cárdenas, A.A., Amin, S., Sastry, S.: Research challenges for the security of control systems. In: Proc. 3rd USENIX Conference on Hot Topics in Security, p. Article 6 (2008)
21. Cárdenas, A.A., Amin, S., Sastry, S.: Secure control: Towards survivable cyber-physical systems. In: Proc. 28th International Conference on Distributed Computing Systems Workshops, pp. 495–500 (2008)
22. Cárdenas, A.A., Amin, S., Sastry, S.: Secure control: Towards survivable cyber-physical systems. In: Proc. First International Workshop on Cyber-Physical Systems (2008)
23. Cárdenas, A.A., Roosta, T., Taban, G., Sastry, S.: Cyber security basic defenses and attack trends. In: Franceschetti, G., Grossi, M. (eds.) Homeland Security Technology Challenges, ch. 4, pp. 73–101. Artech House (2008)
24. Cleveland, F.M.: Cyber security issues for advanced meter infrastructure (AMI). In: Proc. IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century, pp. 1–5 (2008)
25. Constable, G., Somerville, B.: A Century of Innovation: Twenty Engineering Achievements That Transformed Our Lives. Joseph Henry Press, Washington, DC (2003)
26. Conte de Leon, D., Alves-Foss, J., Krings, A., Oman, P.: Modeling complex control systems to identify remotely accessible devices vulnerable to cyber attack. In: Proc. First Workshop on Scientific Aspects of Cyber Terrorism, Washington, D.C. (2002)
27. Dán, G., Sandberg, H.: Stealth attacks and protection schemes for state estimators in power systems. In: Proc. First IEEE International Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, MD, pp. 214–219 (2010)
28. Dán, G., Sandberg, H., Ekstedt, M., Björkman, G.: Challenges in power system information security. IEEE Security & Privacy 10(4), 62–70 (2012)
29. Darby, J., Phelan, J., Sholander, P., Smith, B., Walter, A., Wyss, G.: Evidence-based techniques for evaluating cyber protection systems for critical infrastructures. In: Proc. IEEE Military Communications Conference, pp. 1–10 (2006)
30. Davis, C.M., Tate, J.E., Okhravi, H., Grier, C., Overbye, T.J., Nicol, D.: SCADA cyber security testbed development. In: Proc. 38th North American Power Symposium, pp. 483–488 (2006)
31. Dawson, R., Boyd, C., Dawson, E., Manuel Gonzàlez Nieto, J.: SKMA – A key management architecture for SCADA systems. In: Proc. Fourth Australasian Workshops on Grid Computing and E-Research, vol. 54, pp. 183–192 (2006)
32. Depoy, J., Phelan, J., Sholander, P., Smith, B., Varnado, G.B., Wyss, G.: Risk assessment for physical and cyber attacks on critical infrastructures. In: Proc. IEEE Military Communications Conference, vol. 3, pp. 1961–1969 (2005)

33. Dondossola, G., Garrone, F., Szanto, J.: Supporting cyber risk assessment of power control systems with experimental data. In: Proc. IEEE Power Systems Conference and Exposition, pp. 1–3 (2009)
34. Dörfler, F., Bullo, F.: Synchronization and transient stability in power networks and non-uniform kuramoto oscillators. In: Proc. American Control Conference, pp. 930–937 (2010)
35. Draney, B., Cambell, S., Walter, H.: NERSC cyber security challenges that require doe development and support. Technical Report LBNL–62284, Ernest Orlando Lawrence Berkeley National Laboratory, Berkeley, California (2007)
36. Dudenhoeffer, D.D., Permann, M.R., Woolsey, S., Timpany, R., Miller, C., McDermott, A., Manic, M.: Interdependency modeling and emergency response. In: Proc. 2007 Summer Computer Simulation Conference, pp. 1230–1237 (2007)
37. Eberle, W., Holder, L.: Insider threat detection using graph-based approaches. In: Proc. Cybersecurity Applications and Technology Conference for Homeland Security, pp. 237–241 (2009)
38. Edwards, D., Srivastava, S.K., Cartes, D.A., Simmons, S., Wilde, N.: Implementation and validation of a mult-level security model architecture. In: Proc. International Conference on Intelligent Systems Applications to Power Systems, pp. 1–4 (2007)
39. Ekstedt, M., Sommestad, T.: Enterprise architecture models for cyber security analysis. In: Proc. IEEE Power Systems Conference and Exposition, pp. 1–6 (2009)
40. Falliere, N., Murchu, L., Chien, E.: W32.stuxnet dossier, version 1.3. Symantec (2010)
41. Farris, J.F., Nicol, D.M.: Evaulation of secure peer-to-peer overlay routing for survivable SCADA systems. In: Proc. 36th Conference on Winter Simulation, pp. 300–308 (2004)
42. Fernandez, E.B., Wu, J., Larrondo-Petrie, M.M., Shao, Y.: On building secure SCADA systems using security patterns. In: Proc. 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies (2009)
43. Fleury, T., Khurana, H., Welch, V.: Towards a taxonomy of attacks against energy control systems. In: Second Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection (2008)
44. Flick, T., Morehouse, J.: Securing the Smart Grid: Next Generation Power Grid Security. Syngress (2011)
45. Gellings, C.: The Smart Grid: Enabling Energy Efficiency and Demand Response. Fairmont Press (2009)
46. Giani, A., Karsai, G., Roosta, T., Shah, A., Sinopoli, B., Wiley, J.: A testbed for secure and robust SCADA systems. SIGBED Review 5(2), Article No. 4 (2008)
47. Gilchrist, G.: Secure authentication for DNP3. In: Proc. IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century, pp. 1–3 (2008)
48. Gonen, T.: Electric Power Distribution System Engineering. Mcgraw-Hill College (1985)
49. Grid, N.: Operating the electricity transmission networks in 2020 (2011)
50. GridWise Alliance: GridWise(TM) accelerates efforts to develop a smart grid in the U.S. In: GridWeek, Washington DC, MD (2007)
51. Grochocki, D., Huh, J., Berthier, R., Bobba, R., Sanders, W., Cardenas, A., Jetcheva, J.: AMI threats, intrusion detection requirements and deployment recommendations. In: Proc. Third IEEE International Conference on Smart Grid Communications (SmartGridComm), Tainan, pp. 395–400 (2012)

52. The Cyber Security Coordination Task Group: Smart Grid Cyber Security Strategy and Requirements. National Institute of Standards and Technology
53. Hadeli, H., Schierholz, R., Braendle, M., Tuduce, C.: Generating configuration for missing traffic detector and security measures in industrial control systems based on the system description files. In: Proc. IEEE Conference on Technologies for Homeland Security, pp. 503–510 (2009)
54. HadjSaid, N., Tranchita, C., Rozel, B., Viziteu, M., Caire, R.: Modeling cyber and physical interdependencies – application in ICT and power grids. In: Proc. IEEE Power Systems Conference and Exposition, pp. 1–6 (2009)
55. Hasan, R., Bobba, R., Khurana, H.: Analyzing NASPInet data flows. In: Proc. IEEE Power Systems Conference and Exposition, pp. 1–6 (2009)
56. Holcomb, J.: Auditing cyber security configuration for control system applications. In: Proc. IEEE Conference on Technologies for Homeland Security, pp. 7–13 (2009)
57. Holstein, D.K., Diaz, J.: Cyber security management for utility operations. In: Proc. 39th Annual Hawaii International Conference on Systems Sciences, vol. 10, p. 241c (2006)
58. Hughes, T.: Networks of Power: Electrification in Western Society, 1880-1930. JHU Press (1993)
59. Hull, J., Khurana, H., Markham, T., Staggs, K.: Staying in control: Cyber security and the modern electric grid. IEEE Power & Energy Magazine 10(1), 41–48 (2012)
60. Jones, P.: The role of new technologies: A power engineering equipment supply base perspective. In: Grid Policy Workshop, Paris, France (2010)
61. Kang, D.J., Kim, H.M.: A method for determination of key period using QoS function. In: Proc. Future Generation Communication and Networking, vol. 2, pp. 532–535 (2007)
62. Kang, D.J., Kim, H.M.: A proposal for key policy of symmetric encryption application to cyber security of KEPCO SCADA network. In: Proc. Future Generation Communication and Networking, vol. 2, pp. 609–613 (2007)
63. Khaitan, S., McCalley, S.: Cyber physical system approach for design of power grids: A survey. In: Proc. IEEE Power & Energy Society General Meeting, Vancouver, BC, pp. 1–5 (2013)
64. Khaitan, S., McCalley, S.: Design techniques and applications of cyber physical systems: A survey. IEEE Systems Journal (2014)
65. Khalil, H.: Nonlinear Systems. Prentice-Hall (2002)
66. Khurana, H., Hadley, M., Lu, N., Frincke, D.: Smart-grid security issues. IEEE Security Privacy 8(1), 81–85 (2009)
67. Khurana, H., Khan, M.M.H., Welch, V.: Leveraging computational grid technologies for building a secure and manageable power grid. In: Proc. Hawaii International Conference on System Sciences, pp. 115–124 (2007)
68. Khurana, H., Koleva, R., Basney, J.: Performance of cryptographic protocols for high-performance high-bandwidth and high-latency grid systems. In: Proc. Third IEEE International Conference on e-Science and Grid Computing, pp. 431–439 (2007)
69. Kim, H.M., Kang, D.J., Kim, T.H.: Flexible key distribution for SCADA network using multi-agent system. In: Proc. ECSIS Syposium on Bio-inspired, Learning, and Intelligent Systems for Security, pp. 29–34 (2007)
70. Klein, S.A.: An open source IEC-61850 toolkit for utility automation and wind power applications. In: Proc. IEEE/PES Transmission and Distribution Conference and Exposition, pp. 1–4 (2008)
71. Klein, S.A.: A secure IEC-61850 toolkit for utility automation. In: Proc. Cybersecurity Applications and Technology Conference for Homeland Security, pp. 245–250 (2009)

72. Kosut, O., Jia, L., Thomas, R.J., Tong, L.: Limiting false data attacks on power system state estimation. In: Proc. 44th Annual Conference on Information Sciences and Systems (CISS), Princeton, NJ, pp. 1–6 (2010)
73. Kosut, O., Jia, L., Thomas, R.J., Tong, L.: Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures. In: Proc. First IEEE International Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, MD, pp. 220–225 (2010)
74. Kundur, D.: Cyber-physical security of the smart grid. Lecture conducted from University of Toronto, Toronto, Canada (2013)
75. Kundur, D., Feng, X., Liu, S., Zourntos, T., Butler-Purry, K.: Towards a framework for cyber attack impact analysis of the electric smart grid. In: Proc. IEEE International Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, Maryland, pp. 244–249 (2010)
76. Kundur, D., Feng, X., Mashayekh, S., Liu, S., Zourntos, T., Butler-Purry, K.: Towards modeling the impact of cyber attacks on a smart grid. International Journal of Security and Networks 6(1), 2–13 (2011)
77. Kundur, P.: Power System Stability and Control. McGraw-Hill Professional (1994)
78. Kundur, P.: Power System Stability and Control. McGraw-Hill (1994)
79. Kundur, P., Paserba, J., Ajjarapu, V., Andersson, G., Bose, A., Canizares, C., Hatziargyriou, N., Hill, D., Stankovic, A., Taylor, C., Cutsem, T., Vittal, V.: Definition and classification of power system stability: Ieee/cigre joint task force on stability terms and definitions. IEEE Transactions on Power Systems 19, 1387–1401 (2004)
80. Lin, H., Sambamoorthy, S., Shukla, S., Thorp, J., Mili, L.: Power system and communicaiton network co-simulation for smart grid applications. In: Proc. IEEE PES Conference on Innovative Smart Grid Technologies (ISGT), Anaheim, California, pp. 1–6 (2011)
81. Liu, C.C., Ten, C.W., Govindarasu, M.: Cybersecurity of SCADA systems: Vulnerability assessment and mitigation. In: Proc. IEEE Power Systems Conference and Exposition, pp. 1–3 (2009)
82. Liu, S., Liu, X., El-Saddik, A.: Denial-of-service (DoS) attacks on load frequency control in smart grids. In: Proc. IEEE PES Innovative Smart Grid Technologies (ISGT), Washington DC, MD, pp. 1–6 (2013)
83. Liu, Y., Ning, P., Reiter, M.: Generalized false data injection attacks against state estimation in electric power grids. ACM Transactions on Information and System Security (TISSEC) 14(1) (2011)
84. Liu, Y., Ning, P., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. In: Proc. 16th ACM Conference on Computer and Communications Security, Chicago, IL, pp. 21–32 (2009)
85. Liu, Y., Ning, P., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. ACM Transactions on Information and System Security (2011) (to appear)
86. Mander, T., Nabhani, F., Wang, L., Cheung, R.: Integrated network security protocol layer for open-access power distribution systems. In: Proc. IEEE Power Engineering Society General Meeting, pp. 1–8 (2007)
87. McDaniel, P., McLaughlin, S.: Security and privacy challenges in the smart grid. IEEE Security Privacy 7(3), 75–77 (2009)
88. McMillin, B.: Complexities of information security in cyber-physical power systems. In: Proc. IEEE Power Systems Conference and Exposition, pp. 1–2 (2009)

89. McMillin, B., Gill, C., Crow, M.L., Liu, F., Niehaus, D., Potthast, A., Tauritz, D.: Cyber-physical systems distributed control: The advanced electric power grid. In: Proc. National Workshop on Beyond SCADA: Networked Embedded Control for Critical Physical Systems, HCSS:NEC4CPS (2006)
90. McQueen, M.A., Boyer, W.F.: Deception used for cyber defense of control systems. In: Proc. 2nd Conference on Human System Interactions, pp. 624–631 (2009)
91. McQueen, M.A., Boyer, W.F., Flynn, M.A., Beitel, G.A.: Quantitative cyber risk reduction estimation methodology for small SCADA control system. In: Proc. 39th Annual Hawaii International Conference on Systems Sciences, vol. 9, pp. 226–236 (2006)
92. Meyer, C.D.: Matrix Analysis and Applied Linear Algebra. SIAM (2001)
93. Mohsenian-Rad, A., Leon-Garcia, A.: Distributed internet-based load altering attacks against smart power grids. IEEE Transactions on Smart Grid 2(4), 667–674 (2011)
94. Moslehi, K., Kumar, R.: A reliability perspective of the smart grid. IEEE Transactions on Smart Grid 1(1), 57–64 (2010)
95. Olfati-Saber, R.: Flocking for multi-agent dynamic systems: Algorithms and theory. IEEE Transactions on Automatic Control 51(3), 401–420 (2006)
96. Olfati-Saber, R., Fax, J., Murray, R.: Consensus and cooperation in networked multi-agent systems. Proceedings of the IEEE 95(1), 215–233 (2007)
97. Patel, S.C., Bhatt, G.D., Graham, J.H.: Improving the cyber security of SCADA communication networks. Communications of the ACM 52(7), 139–142 (2009)
98. Piètre-Cambacédès, L., Sitbon, P.: Cryptographic key management for SCADA systems – issues and perspectives. In: Proc. International Conference on Information Security and Assurance, pp. 156–161 (2008)
99. Reynolds, C.: Flocks, herds, and schools: a distributed behavioral model. Computer Graphics 21(4), 25–34 (1987)
100. Risley, A., Carson, K.: Low- or no-cost cybersecurity solutions for defending the electric power system against electronic intrusions. Schweitzer Engineering Laboratories, Inc. (2006)
101. Rozel, B., Viziteu, M., Caire, R., Hadjsaid, N., Rognon, J.P.: Towards a common model for studying critical infrastructure interdependencies. In: Proc. IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, Pennsylvania, pp. 1–6 (2008)
102. Sauer, P., Pai, M.: Power System Dynamics and Stability. Prentice Hall (1997)
103. Sioshansi, F.: Smart Grid: Integrating Renewable, Distributed & Efficient Energy. Academic Press (2011)
104. Sologar, A., Moll, J.: Developing a comprehensive substation cyber security and data management solution. In: Proc. IEEE/PES Transmission and Distribution Conference and Exposition, pp. 1–7 (2008)
105. Sou, K., Sandberg, H.: Detection and identification of data attacks in power system. In: American Control Conference (ACC), Montreal, QC, pp. 3651–3656 (2012)
106. Stamp, J., McIntyre, A., Ricardson, B.: Reliability impacts from cyber attack on electric power systems. In: Proc. IEEE Power Systems Conference and Exposition, pp. 1–8 (2009)
107. Takano, M.: Sustainable cyber security for utility facilities control system based on defense-in-depth concept. In: Proc. SICE Annual Conference, pp. 2910–2913 (2007)
108. Tan, H.: Security analysis of a cyber-physical system. Master's thesis, University of Missouri-Rolla (2007)
109. Tang, H., McMillin, B.: Security property violation in CPS through timing. In: Proc. 28th International Conference on Distributed Computing Systems Workshops, pp. 519–524 (2008)

110. Ten, C.W., Liu, C.C., Govindarasu, M.: Vulnerability assessment of cybersecurity for SCADA systems using attack trees. In: Proc. IEEE Power Engineering Society General Meeting, pp. 1–8 (2007)
111. Ton, D.: DOE's perspectives on smart grid technology, challenges, & research opportunities. In: UCLA Engineering SmartGrid Seminar, Los Angeles, CA (2009)
112. Tuzzo, S.: A PlugN'Play platform independent solution that eliminates unauthorized access without the use of passwords or encryption keys. In: Proc. IEEE Conference on Technologies for Homeland Security, pp. 79–85 (2008)
113. Vijayan, J.: Stuxnet renews power grid security concerns. Computerworld (2010)
114. Wang, Y., Chu, B.T.: sSCADA: Securing SCADA infrastructure communications (2004), http://eprint.iacr.org/2004/265.pdf
115. Wei, J., Kundur, D.: A multi-flock approach to rapid dynamic generator coherency identification. In: Proc. IEEE Power & Energy Society General Meeting, Vancouver, Canada, pp. 1–5 (2013)
116. Wei, J., Kundur, D., Zourntos, T.: On the use of cyber-physical hierarchy for smart grid security and efficient control. In: Proc. IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Montreal, Canada (2012)
117. Wei, J., Kundur, D., Zourntos, T., Butler-Purry, K.: A flocking-based dynamical systems paradigm for smart power system analysis. In: Proc. IEEE Power & Energy Society General Meeting, San Diego, California (2012)
118. West, A.: Securing DNP3 and Modbus with AGA12-2J. In: Proc. IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century, pp. 1–4 (2008)
119. Xiangjun, Z.: Context information-based cyber security defense of protection system. IEEE Transactions on Power Delivery 22(3), 1477–1481 (2007)
120. Xiao, K., Chen, N., Ren, S., Shen, L., Sun, X., Kwiat, K., Macalik, M.: A workflow-based non-intrusive approach for enhancing the survivability of critical infrastructures in cyber environment. In: Proc. Third International Workshop on Software Engineering for Secure Systems (2007)
121. Xie, L., Mo, Y., Sinopoli, B.: False data injection attacks in electricity markets. In: Proc. IEEE International Conference on Smart Grid Communications, Tainan, Taiwan, pp. 226–231 (2010)
122. Yamada, T., Maruyama, T.: Study on a security framework for a plant level network. In: Proc. 2006 SICE-ICASE International Joint Conference, Bexco, Busan Korea, pp. 1063–1066 (2006)