Probing the Telltale Physics: Towards a Cyber-Physical Protocol to Mitigate Information Corruption in Smart Grid Systems

Jin Wei, Deepa Kundur, Takis Zourntos and Karen Butler-Purry

Department of Electrical & Computer Engineering
Texas A&M University, College Station, TX 77843, USA

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

I. Introduction

The smart grid boasts higher reliability, efficiency and consumer-centricity in an environment of increasing power demand through the effective use of information – namely, information about the right thing, to the right party, at the right time. The acquisition, transmission and consumption of high-granularity real-time power system data is facilitated through the integration of communications, computing and advanced control technologies. Such dependence on information technology naturally raises questions as to the effects of information corruption on power system operation.

Recent work focused on false data injection attacks has demonstrated how an opponent can bias power system measurements and overcome residual-based bad data detection approaches [1]. Subsequent research has focused on identifying such attacks [2]–[4] and has largely taken an information perspective. More recently, the smart grid security community has been considering cyber-physical perspectives [5]. In this paper, 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. We build on our past work on a flocking-based modeling paradigm for power system transient stability and control [6], [7] to 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 is in contrast to our prior work that has assumed all PMU data is accurate.

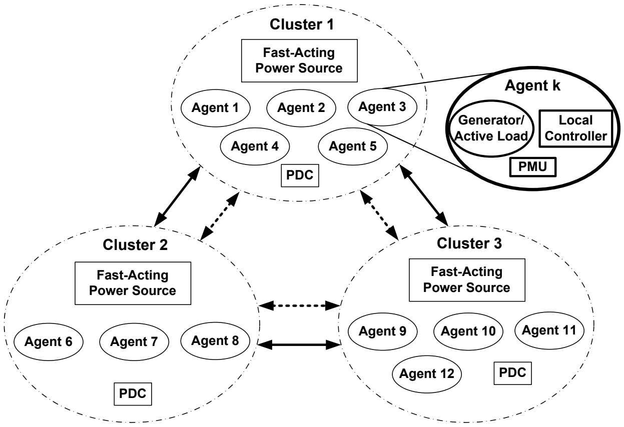


Fig. 1. Proposed two-tier hierarchical cyber-physical integrated communication framework; solid (dashed) lines with arrows represent physical (cyber) couplings. Detailed structure for each agent given.

In the next section, we present our problem framework. Section III introduces our flocking-based smart grid modeling paradigm with novel hierarchical system dynamics. Section IV proposes our original witness-based security protocol to mitigate cyber corruption. Simulation results and final remarks are presented in Sections V and VI, respectively.

II. Problem Setting

We consider the two-tier hierarchical cyber-physical multi-agent framework of Fig. 1 to model the transient stability problem in a smart grid system. As illustrated, our model consists of *clusters* of *agents*. Each *agent* consists of: (1) a dynamic node representing a power system generator, (2) a phasor measurement unit (PMU) that acquires information including the rotor angle and frequency of the associated generator, and (3) a local cyber-controller that employs PMU data from select generators to compute a control signal that is applied to the local generator of the same agent.

In the face of a cyber of physical disturbance a natural frequency-based grouping of generators ensues whereby agents corresponding to generators within a collection are said to exhibit high physical coherence and form a state-dependent *cluster*. As such, a cluster consists of generator agents with high physical coherence, a phasor data concentrator (PDC) that represents a PMU communications gateway, and a fast-acting power source employed by local controllers for system stabilization through power injection/absorption at generator buses as discussed in [8]. The agent with the highest inertia generator in a cluster is termed the *lead* agent while the others are referred to as secondary. Inter-cluster PMU communications involves data exchange amongst lead agent PMUs through a multi-hop network consisting of source/sink nodes which are the lead agents' PDCs. Intra-cluster PMU communications occurs through a local area network (LAN) whereby the PDC acts as an aggregator. The PDC also aligns the PMU data prior to sending information to a local controller.

In [7], the authors presented a two-tier hierarchical smart grid protection framework, which exploits generator coherence to activate local cyber control only at lead generators of clusters. Moreover, it is shown that only lead agent PMU information is needed to ensure transient system stabilization in the face of a disturbance (even if the fault is cleared after the critical clearing time (CCT)). The objective of the active controllers is to achieve lead agent frequency synchronization in the face of cyber-physical disturbance. The secondary generators achieve synchronization via strong physical couplings with a stabilized lead generator. The resulting adaptive cyber-physical system exhibits a hierarchical structure whereby inter-cluster interactions are cyber-physical (tier-1) and intra-cluster synergies are physical (tier-2). A natural question arises as to the effects of lead agent PMU data corruption on the transient stabilization capabilities of the system.

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

III. Flocking-Based Cyber-Physical Modeling

A. Modeling of Transient Stability

To describe the *physical* power system, we make use of the well-known interconnected swing equations to describe rotor dynamics of the Kron-reduced power system as detailed by Dörfler and Bullo in [9] to give the following dynamical representation for each agent:

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

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 relative normalized frequency, $M_i > 0$ and $D_i > 0$ represent the generator inertia and the damping parameters, respectively, 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.

It has been shown that Eq. (1) can be compactly represented, via singular perturbation analysis, as [10]:

$$\mathbf{D}\dot{\boldsymbol{\omega}} = -\mathbf{L}\boldsymbol{\omega}, \quad (2)$$

where $\mathbf{D} = \text{diag}\,[D_1, D_2, \ldots, D_N]$, $\boldsymbol{\omega} = [\omega_1, \ldots, \omega_N]^T$, $\mathbf{L}$ is a $N \times N$ matrix whose elements l_{ij} are defined as:

$$l_{ij} = \begin{cases} -P_{ij}\cos(\theta_i - \theta_j + \varphi_{ij}), & \text{if } i \neq j \\ \sum_{k=1}^{N-1} P_{ik}\cos(\theta_i - \theta_k + \varphi_{ik}), & \text{otherwise} \end{cases} \quad (3)$$

assuming overdamped generators, $D_i \gg M_i$; we later relax this constraint in our flocking-based framework.

It is well-known that transient stability describes the ability of a power system to remain in synchronism when subjected to large disturbances such as transmission line faults and generator loss [11]. Achieving transient stability in a faulted system consists of maintaining both exponential frequency synchronization and phase angle cohesiveness after the fault is cleared. In the context of the model of Eq. 2, exponential frequency synchronization requires the frequencies of the generators to agree asymptotically to a common value set to 60 Hz (normalized to 0) in North America; i.e., $\omega_i(t) \to 0, \ as \ \ t \to \infty$ for all i. Phase angle cohesiveness necessitates that the difference between the phase angle of each generator the center of inertia (COI) of all phases should be below a pre-defined threshold typically chosen as 100°; i.e., $|\theta_i(t) - \theta_{COI}(t)| \leq \gamma, \forall\ t$ where $\gamma \approx 100°$.

It can be shown via continuity arguments that the time-varying matrix $\mathbf{L}$ can be interpreted as the Laplacian (with zero row-sum and positive semi-definite (PSD) character) of a directed weighted graph $\mathcal{G}$ associated with the power system topology for a small time interval after the fault is cleared; the associated weight of an edge e_{ij} in $\mathcal{G}$ would be given by l_{ij}. Thus, the ability of the physical power system to achieve transient stability is largely dependent on the characteristics of $\mathbf{L}$ post-fault-clearing. If clearing occurs after the critical clearing time (CCT), then $\mathbf{L}$ will eventually lose its PSD nature commonly resulting in transient instability. Otherwise, $\mathbf{L}$ will remain PSD providing transient stability.

Our approach to hierarchical system protection employs the matrix $\mathbf{L}$ to determine physically coherent generators to form state-dependent clusters as summarized in the next section. Then, cyber-control is applied only at the lead generators of clusters to reinforce the physical links to ensure that the *effective* Laplacian of the overall cyber-physical system is PSD and hence guarantee transient stability. This approach borrows tools from flocking theory as we discuss in Section III-C.

B. Cluster Formation and Control

It is well known that for Laplacian matrices, the second smallest eigenvalue λ_2 represents the algebraic connectivity of its associated graph. Moreover, we employ the signs of the elements of the associated eigenvector $\mathbf{v}$ (called the Fiedler vector) to provide information for *spectral bisection* [12] to partition $\mathcal{G}$ into two relatively disjoint (in terms of physical coupling) subgraphs. In the case of bisection, one group of generators will represent high coherency and the other low. We assume, as typical, that the number of generator groups to partition through repeated application of bisection is known a priori and denoted C. Details are provided in [6], [7].

After the clusters are established, the agent whose generator has the highest inertia is selected as the lead agent and assigned an index i. To reduce PMU communication overhead, only the lead agents communicate with each other through the multi-hop inter-cluster network to compute the control u_i. The control signal is used to actuate a fast-acting power source $P_{u,i}$ (such as a battery) that tracks u_i to provide power injection (for $u_i > 0$) or absorption (for $u_i < 0$) at the associated generator bus. Typically PMU data for computation of u_i will be delayed during transmission through the inter-cluster network. Incorporating a latency of τ, we therefore represent the overall cyber-physical coupling as:

$$\begin{aligned} M_i\dot{\omega}_i = \; & -D_i\omega_i + P_{m,i} - |E_i|^2 G_{ii} \\ & - \sum_{j=1}^{N} P_{ij}\sin(\theta_i - \theta_j + \varphi_{ij}) + \alpha_i u_{i,\tau}. \end{aligned} \tag{4}$$

where $i = 1, \cdots, N$, N denotes the number of agents, $\alpha_i = 1$ if the ith agent is a lead agent and $\alpha_i = 0$ otherwise, and the cyber-control signal is equal to $u_i = P_{u,i}$ with the time delay τ caused mainly by queuing delays [13]. As mentioned in Section II, the PDCs help to guarantee the synchronization of the PMU information from the various lead agents, and thus a consistent delay τ is experienced by all cyber information.

C. Flocking-Based Hierarchical Communications Framework

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 [14], [15], the authors 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.

Inspired by the analogies present between the requirements for transient stability and these flocking rules, we developed a flocking-based control protocol with the cyber-control signal $\mathbf{u}$ consisting of four terms: a *gradient-based term* to ensure phase angles of all synchronous generators are within 100^o required for transient stability, a *consensus term* to enable frequencies of all generators converge, *navigation feedback* so that frequencies converge to 60 Hz and a component designed to enable singular perturbation analysis [8].

Given C is the number of clusters in our hierarchical communication framework, we reorder our index assignments so that Agents $i = 1, \ldots, C$ correspond to lead agents. We have shown that the following flocking-inspired control assignment provides transient stability [8]:

$$\widetilde{\mathbf{u}} = \dot{\mathbf{u}} = -\mathbf{B}\dot{\boldsymbol{\omega}} - \nabla\mathbf{V} - \mathbf{G}\boldsymbol{\omega} - c_1(\boldsymbol{\omega} - \boldsymbol{\omega}^*) \tag{5}$$

where $\dot{\mathbf{u}}$ is the time-dervative of $\mathbf{u}$, $\boldsymbol{\omega} = [\omega_1, \ldots, \omega_C]^T$ (note that this is distinct from that original definition of Eq. (2)), $\mathbf{B}$ is a $C \times C$ cyber coupling matrix designed to relax the over-damped generator assumption, $\mathbf{G}$ is another $N \times N$ cyber coupling matrix designed to achieve frequency consensus, $\nabla\mathbf{V}$ is the gradient-based term, c_1 is the parameter for the linear navigational feedback and $\boldsymbol{\omega}^* = \mathbf{0}$ is the desired relative normalized generator frequency.

In our proposed hierarchical communication framework, the agents within a cluster exhibit high coherence, thus we propose to estimate the states of the secondary agents as "noisy" versions of those of the lead agents. Therefore, we estimate the state of the ith secondary agent (θ_i, ω_i) belonging to the cluster with Lead Agent k as follows:

$$\begin{cases} \widehat{\omega}_i = \omega_k + \varepsilon_i, \\ \widehat{\theta}_i = \theta_k + \Delta\theta_{ik} + \varsigma_i, \end{cases} \tag{6}$$

where $\Delta\theta_{ik}$ denotes the phase angle difference between the ith and kth agents in the static (pre-fault) state, and $\varepsilon_i \sim \mathcal{N}(0, \mu)$ and $\varsigma_i \sim \mathcal{N}(0, \sigma)$ are zero-mean Gaussian random variables with $\mu \ll 1$ and $\sigma \ll 1$. Using Eq. (6) and neglecting noise, we estimate $\mathbf{L}$ of Eq. (3) and denote the result $\widetilde{\mathbf{L}}$.

Therefore, combining Eqs. (4) and (5) and singular perturbation analysis, our flocking-based hierarchical cyber-physical communication framework is represented as:

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

$$\begin{cases} \dot{\boldsymbol{\theta}} = \boldsymbol{\omega}, \\ \mathbf{W}\dot{\boldsymbol{\omega}} = -(\mathbf{R} + \mathbf{S}\Psi)\,\boldsymbol{\omega} - \mathbf{S}\boldsymbol{\varepsilon} - \nabla\mathbf{V}_\tau - \mathbf{G}_\tau\boldsymbol{\omega}_\tau - c_1\boldsymbol{\omega}_\tau, \end{cases} \tag{7}$$

where the subscript τ denotes cyber delay, $\mathbf{W} = \mathbf{B} + \mathbf{D}$, $\mathbf{D} = \text{diag}\,[D_1, \ldots, D_C]$, $\boldsymbol{\varepsilon} = [\varepsilon_{C+1}, \cdots, \varepsilon_N]^T$, $\mathbf{R}$ and $\mathbf{S}$ are the partitions of $\widetilde{\mathbf{L}}$ as follows:

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

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

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

$$\begin{cases} \dot{\boldsymbol{\theta}}_l = \boldsymbol{\omega}_l, \\ \mathbf{D}\dot{\boldsymbol{\omega}}_l = -\mathbf{L}\boldsymbol{\omega}_l - \mathbf{M}\ddot{\boldsymbol{\omega}}_l, \end{cases}$$

where $\mathbf{M} = \text{diag}\,[M_{C+1}, \ldots, M_N]$, $\boldsymbol{\theta}_l = [\theta_{C+1}, \cdots, \theta_N]^T$, and $\boldsymbol{\omega}_l = [\omega_{C+1}, \cdots, \omega_N]^T$.

IV. Witness-Based Security Protocol

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

Table I
PROPOSED CYBER-PHYSICAL VERIFICATION SCHEME

```
Let the lead agent PMU reading be $\theta^c$. Let the secondary agents be
represented with indices from the set $i \in \mathcal{I}$ and their readings be denoted
$\theta_i$. Let $\Delta\theta_i$ be the phase angle difference between $\theta_i$ and $\theta^c$ at static state
(i.e., pre-fault). We assign $H_k = |\mathcal{I}| + 1$.
1. Initialize $Count = 0$ and set the threshold $\tau_p$.
2. For each $i \in \mathcal{I}$
      $\xi_i = \theta_i - \Delta\theta_i - \theta^c$,
      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 II
PROPOSED CYBER-PHYSICAL ESTIMATION SCHEME

```
Let the secondary agents be represented with indices from the set $i \in \mathcal{I}$.
Let $\boldsymbol{\xi_i} \in \mathbb{R}^{\ell}$ be a vector containing the $\ell$ most recent sample values of
$\xi_i$ in chronological order. Let $a(n)$ be an $\ell$-point Hamming window.
1. For each $i \in \mathcal{I}$
      Secondary agent estimates lead agent phase angle using Eq. (6).
      Secondary agent reports the estimation result $\widehat{\theta}_i^c$ to the PDC.
   End
2. The PDC evaluates estimation accuracy for $i \in \mathcal{I}$ by computing:
      $$\widehat{\sigma}_i = \sqrt{\frac{\sum_{n=1}^{\ell} a(n-1)\boldsymbol{\xi_i}(n)^2}{\sum_{n=1}^{\ell} a(n-1)}}. \quad (8)$$
3. The PDC forms $\widehat{\boldsymbol{\theta}}_{\boldsymbol{l}}$ consisting of elements $\widehat{\theta}_i^c, i \in \mathcal{I}$ ordered to reflect
   monotonically increasing values in $\widehat{\sigma}_i$.
4. The PDC estimates $\theta^c$ from a median-like value from the elements
   of $\widehat{\boldsymbol{\theta}}_{\boldsymbol{l}}$ to avoid extreme biases:
$$\widehat{\theta}^c = \begin{cases} \widehat{\boldsymbol{\theta}}_{\boldsymbol{l}}\left(\frac{1}{2}H_k\right), & \text{if } H_k \text{ is even;} \\ \frac{1}{2}\left[\widehat{\boldsymbol{\theta}}_{\boldsymbol{l}}\left(\frac{1}{2}(H_k-1)\right) + \widehat{\boldsymbol{\theta}}_{\boldsymbol{l}}\left(\frac{1}{2}(H_k-1)+1\right)\right], & \text{otherwise} \end{cases}$$
```

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

As described in Eq. (6), 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 I. Since our proposed flocking-based control protocol is robust to the biases on the measurement of the lead agents' frequency [16], 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 $\{\xi_i | i \in \mathcal{I}\}$ for possible future estimation use. Otherwise, it estimates the true value using the proposed cyber-physical estimation scheme of Table II. 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. (7) is guaranteed analytically [7], but witness-based protocol performance is studied empirically.

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

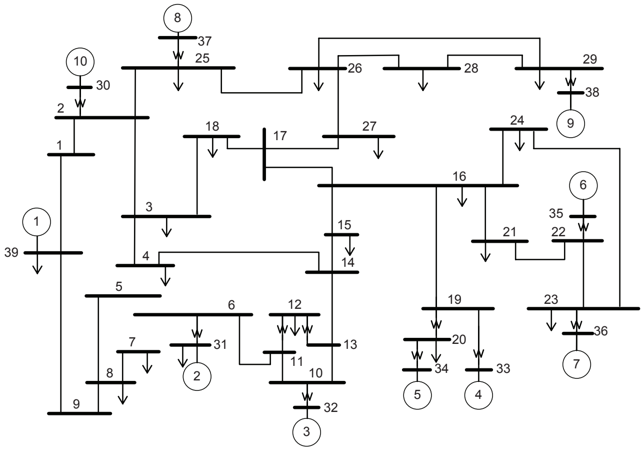
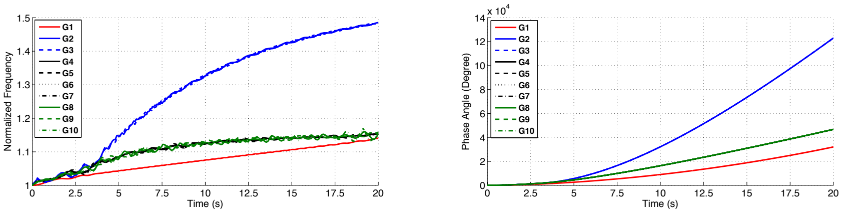


Fig. 2. New England 39-bus power system,

V. SIMULATIONS

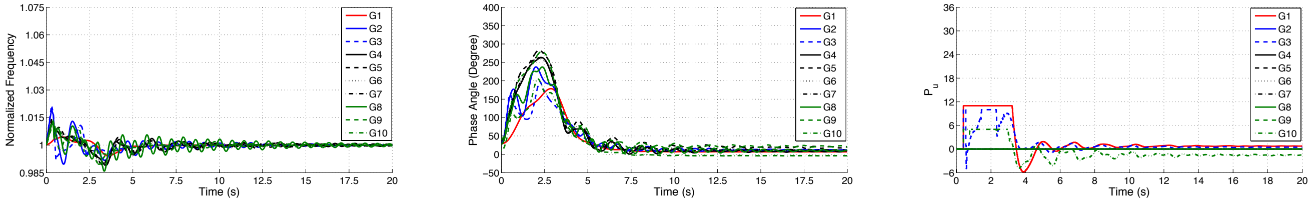
We simulate the 39-bus New England test system of Fig. 2 using MATLAB/Simulink whereby a 3-phase fault occurs at Bus 14 at $t = 0$ s and Line 14-15 is opened at time $t = 0.3$ s (after the CCT of 0.09 s). Fig. 3 shows the rotor frequencies and the phase angles over a period of 20 s when no control is applied. Instability is clearly evident.

Our spectral bisection-based approach for cluster identification is achieved at $t = 0.35$ s; we conclude that the physical system can be effectively modeled with $C = 3$ clusters with groupings: $\{\text{Agent } 1\}$, $\{\text{Agent } 2, \text{Agent } 3\}$, and



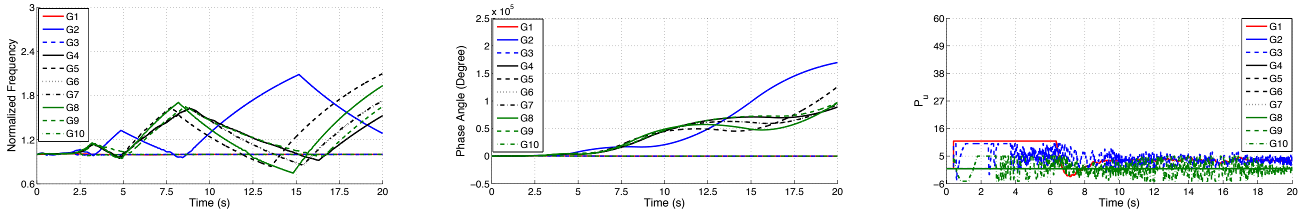
(a) Normalized rotor frequencies versus time. (b) Phase angles versus time.

Fig. 3. Normalized rotor frequencies and phase angles versus time without active control.



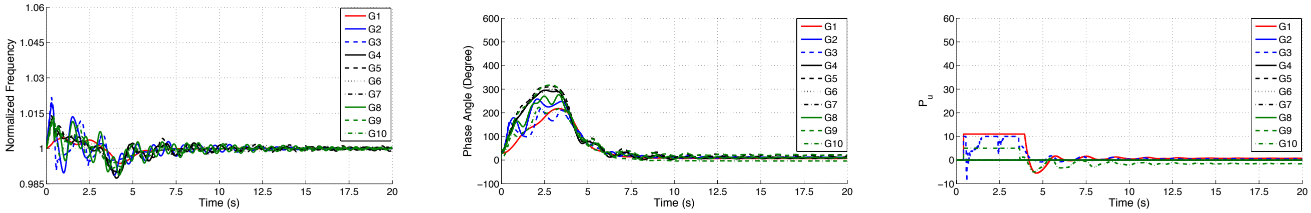
(a) Normalized rotor frequencies versus time. (b) Phase angles versus time. (c) Injected power P_u versus time.

Fig. 4. Normalized rotor frequencies, phase angles, and P_u with proposed cyber-physical control and security protocol when there is no attack.



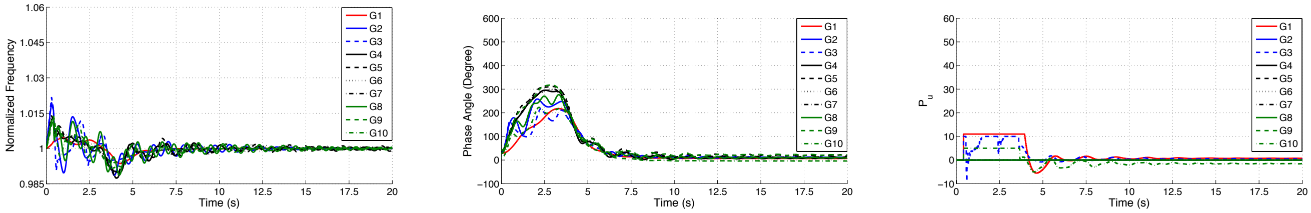
(a) Normalized rotor frequencies versus time. (b) Phase angles versus time. (c) Injected power P_u versus time.

Fig. 5. Normalized rotor frequencies, phase angles, and P_u without proposed cyber-physical security protocol in presence of random attack.



(a) Normalized rotor frequencies versus time. (b) Phase angles versus time. (c) Injected power P_u versus time.

Fig. 6. Normalized rotor frequencies, phase angles, and P_u with proposed cyber-physical security protocol in presence of random attack.



(a) Normalized rotor frequencies versus time. (b) Phase angles versus time. (c) Injected power P_u versus time.

Fig. 7. Normalized rotor frequencies, phase angles, and P_u with proposed cyber-physical security protocol in presence of smart attack.

$\{\text{Agent } 4, \text{Agent } 5, \text{Agent } 6, \cdots, \text{Agent } 10\}$. The lead agents, selected as having the highest inertia generator for each cluster, are given by: Agents 1, 3 and 10. The cyber-control is activated for each lead generator at $t = 0.4$ s which computes $u_i = P_{u,i}$ for each lead agent. A maximum limit on the amount of power injected at each generator bus by the fast reacting grid is assumed such that $P_{u,i}/P_{r,i} \leq 1$ where $P_{r,i}$ is the rated power such that clipping of the control occurs. In our simulation, 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, $\ell = 50$ and the end-to-end latency of the wide-area multi-hop network is designated 0.012 s. The threshold $\tau_p = 35°$. Figs. 4 (a) and (b) present the normalized system frequency and phase, respectively, in the presence of the flocking-based communications and control applied at $t = 0.4$ s and when there is no cyber attack. The injected power is shown in Fig. 4 (c) and demonstrates clipping for Agents 1, 3 and 10.

Figure 5 shows the normalized rotor frequencies, phase angles and P_u in the presence of "random" bias attack when no witness-based cyber protection is applied. The attack specifically consists of PMU corruption of Agents 6, 9 and 10 at $t = 1$ s for duration 1 s, 2 s, and 1.5 s with biases $114.6°$, $-171.9°$, and $-257.8°$, respectively. From Fig. 5, 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. Figure 6 shows 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. Transient stability is still maintained in the presence of the random attack.

Figure 7 addresses the situation in which the compromised PMUs of Agent 6, 9 and 10 collude and report the same biased readings (bias = $-257.8°$) starting at $t = 1$ s for duration 1 s, 2 s, and 1.5 s, respectively. Both protocols are applied. Figure 7 demonstrates that our proposed security protocol is still robust to this type of collusion since the number of corrupted PMU measurements $\ell = 3$ is less than or equal to $\lfloor \frac{1}{2} H_k \rfloor$ where $H_k = 7$, which obeys our threat model of Section IV.

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 power system's transient stability. The simulation results also help demonstrate robustness against attacks on the secondary agents' PMUs as long as our threat model of Section IV is satisfied.

VI. Conclusions

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

We assert that the strength of our scheme is in the effective use of state-dependent hierarchy. Information is exploited to provide a novel distributed control paradigm for smart grid transient stability in the presence of physical disturbances while physical coherence is leveraged so that information can be selectively used for robustness to cyber attack. Future work will examine a generalized class of threat models for which our approach is able to identify data corruption.

VII. Acknowledgements

Research funding was provided by the U.S. National Science Foundation under grant ECCS-1028246 and the Norman Hackerman Advanced Research Program Project Number 000512-0111-2009.

References

[1] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conference on Computer and Communications Security*, Chicago, IL, November 2009, pp. 21–32.

[2] R. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on DC state estimation," in *Proc. First Workshop on Secure Control Systems*, Stockholm, Sweden, April 2010.

[3] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proc. First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Gaithersburg, MD, October 2010, pp. 214–219.

[4] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "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, October 2010, pp. 220–225.

[5] Y. Mo, T. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopol, "Cyber-physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, January 2012.

[6] J. Wei and D. Kundur, "Two-tier hierarchical cyber-physical security analysis framework for smart grid," in *Proc. IEEE Power Engineering Society General Meeting*, 2012.

[7] J. Wei, D. Kundur, and T. Zourntos, "On the use of cyber-physical hierarchy for smart grid security and efficient control," in *IEEE Canadian Conference on Electrical and Computer Engineering*, 2012.

[8] J. Wei, D. Kundur, T. Zourntos, and K. Butler-Purry, "A flocking-based dynamical systems paradigm for smart power system analysis," in *Proc. IEEE Power Engineering Society General Meeting*, 2012.

[9] F. Dörfler and F. Bullo, "Synchronization and transient stability in power networks and non-uniform kuramoto oscillators," in *Proc. American Control Conference*, June-July 2010, pp. 930–937.

[10] ——, "Topological equivalence of a structure-preserving power network model and a non-uniform Kuramoto model of coupled oscillators," in *Proc. IEEE Conference on Decision and Control and European Control Conference*, Orlando, FL, December 2011, pp. 7099–7104.

[11] P. Kundur, *Power System Stability and Control*. McGraw-Hill, 1994.

[12] A. Seary and W. Richards, *Dynamic Social Network Modeling and Analysis*. National Academies' Press, 2003.

[13] P. Kansal and A. Bose, "Smart grid communication requirements for the high voltage power system," in *Proc. IEEE Power Engineering Society General Meeting*, 2011.

[14] C. Reynolds, "Flocks, herds, and schools: a distributed behavioral model," *Computer Graphics*, vol. 21, no. 4, pp. 25–34, July 1987.

[15] I. D. Couzin, J. E. N. S. Krause, R. James, G. D. Ruxton, and N. R. Franks, "Collective momory and spatial sorting in animal groups," in *Journal of Theoretical Biology*, 2002.

[16] R. Olfati-Saber, J. Fax, and R. Murray, "Consensus and cooperation in networked multi-agent systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 215–233, January 2007.