A Flocking-Based Model for DoS-Resilient Communication Routing in Smart Grid

Jin Wei and Deepa Kundur
Department of Electrical & Computer Engineering
Texas A&M University, College Station, TX 77843, USA

***Abstract*—We study the modeling of communication routing strategies in wide area monitoring systems based on flocking theory. We assert that analogies exist between the flocking principles of behavioral transitions, collision avoidance and obstacle avoidance and the routing goals of adaptability, buffer overflow management and re-routing in the presence of changing network conditions. Our model is dynamic and can easily be incorporated in existing flocking-based models of power system operation to provide an overall hierarchical cyber-physical model for a smart grid. Through simulations we show how our model can provide insight on effective routing strategies to promote the transient stabilization of faulted power systems in the presence of denial-of-service attacks on communications infrastructure.**

I. Introduction

Power system 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 [1]. For smart grid systems, achieving transient stability consists of maintaining both *exponential frequency synchronization* and *phase angle cohesiveness* of its generators through application of distributed control. Such protection strategies must therefore make use of information from phasor measurement units (PMUs) of the associated wide area monitoring system. This strongly couples the success of power system control and operation to the ability of the underlying communication network to fulfill stringent timing guarantees.

In this paper we aim to study the interaction of communication network routing with the ability of distributed control mechanisms to maintain transient stability. Such a model must account for varying PMU data rate (and subsequent network congestion) as a function of power systems state; in a "stressed" power system state the PMU data rate will likely be increased to enable advanced compensation strategies. It must also model communication delays due to congestion and attacks such as denial-of-service (DoS) and its effect on power system operation. We build upon our past work on modeling the interaction between distributed control and physical power system elements to include the varying dynamics of communication systems [2], [3]. Specifically, we conveniently employ biological models based on flocking theory.

A. Flocking for Transient Stability

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. Flocking behavior has been described by a set of heuristic agent-interaction rules [4], [5]:

1) *Flock Centering*: agents attempt to stay close to nearby flockmates,
2) *Velocity Matching*: agents attempt to match velocity with nearby flockmates,
3) *Goal Seeking*: each agent has a desired velocity towards a specified position in global space,
4) *Behavioral Transitions*: the history of an agent's state influences future collective behavior,
5) *Collision Avoidance*: agents avoid collisions with nearby flockmates,
6) *Obstacle Avoidance*: agents avoid obstacles by steering away from approaching their goals.

Recently, the authors proposed an approach to flocking-based distributed control for transient stability of smart power systems [2] that made use of the first three interaction rules. Analogies of *flock centering* to phase angle cohesiveness, and *velocity matching* and *goal seeking* to exponential frequency synchronization were established to reformulate the transient stability problem into one of flocking-based multi-agent control. The cyber-physical control was computed from PMU information of other generators and was implemented with the use of an external fast-reacting power source injected at the corresponding generator bus. To minimize communication and control overhead, a state-dependent hierarchical framework was proposed by the authors in [3] whereby agents with high coherence generators were clustered such that only a "lead" agent from the cluster was activated for communications and control while the "secondary" agents were naturally regulated through their tight physical coupling with their associated lead.

In this work, we extend or model to include the dynamics associated with communication networking over a multi-hop mesh network. Specifically we leverage the latter three flocking principles of *behavioral transitions*, *collision avoidance* and *obstacle avoidance* to model communication network routing strategies. We assert that the resulting cyber-physical system model enables the study and design an overall smart grid that is resilient to both physical faults and DoS attacks.

II. Problem Setting

We model the cyber-physical interactions within the smart grid via the two-tier hierarchical multi-agent-based framework of Fig. 1. Here, an agent consists of both cyber and physical

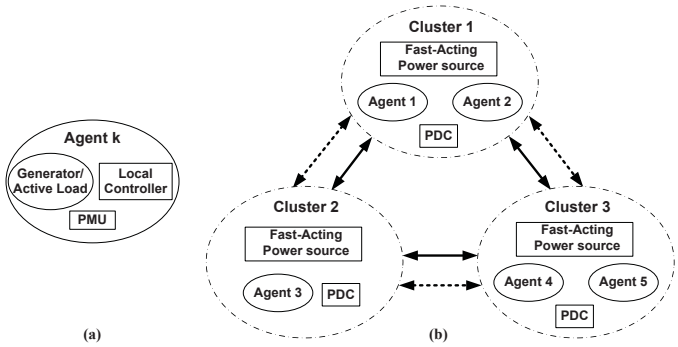

Fig. 1. Solid (dashed) lines with arrows represent physical (cyber) couplings. (a) Agent structure, (a) Proposed two-tier hierarchical multi-agent dynamic system model.

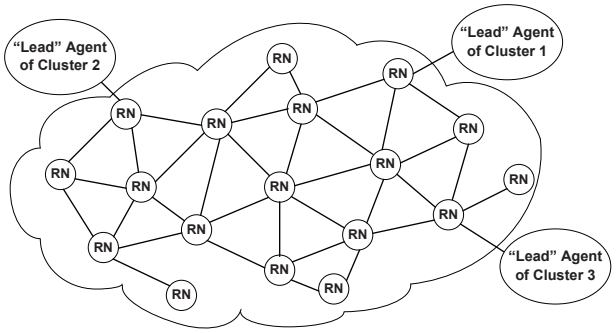

Fig. 2. Wide-area multi-hop mesh network for PMU communications.

elements: (1) a dynamic (physical) generator node, (2) a (cyber) PMU that acquires data such as phase angle and frequency from the generator node, and (3) a local (cyber) controller that, if activated, obtains information from its PMU and others to compute a control signal that is applied to the generator node of the same agent. An agent's frequency, phase angle and coherency with other agents are determined by that of its generator. The state-dependent hierarchy is established as a way to group agents of generators with high physical coherency together to form a *cluster*. One "lead" agent within a cluster is selected such that only its PMU and local controller are activated for overall cluster regulation. Thus as illustrated in Fig. 1(b), inter-cluster interactions are cyber-physical (tier-1) and intra-cluster synergies are physical (tier-2).

Our application focus in this paper is to maintain transient stability in the face of cyber-physical disturbance through distributed control that employs fast-reacting external power sources to achieve generator frequency synchronization. As such, each cluster includes external source(s) such as battery storage, renewables, plug-in hybrid electric vehicles (PHEVs) and flywheels and a phasor data concentrator (PDC) to guarantee synchronization of the data flows amongst lead agents. The effective information (cyber) and power (physical) flows shown via dashed and solid arrows in Fig. 1(b) are realized by the power network and wide-area multi-hop network of Fig. 2.

As shown in Fig. 2, the lead agents exchange PMU data through a multi-hop mesh network recently studied for smart grid communications [6]–[8]. The network consists of lead agents representing sources and sinks, relay nodes (RNs) and finite capacity communication links. In order to enable real-time guarantees of the time-critical PMU data flow in the face of network attack, we propose and model the use of a self-adaptable bidirectional routing protocol over the multi-hop network, which is the focus of this paper.

A. Hierarchical Flocking-Based Cyber-Physical Control

The focus of this paper is on the modeling of information flows through multi-hop routing within the smart grid system of Fig. 1. Thus we refer the reader to [2] and [3] for in-depth development of the power flow counterpart, a hierarchical flocking-based dynamical systems model. Here, we provide a brief overview.

Our dynamical systems model for power flow makes use of a Kron-reduced topology of the power system that employs the swing-equation model for each synchronous generator. Such a physical model has been recently employed to equate the transient stability mode in a power network to synchronization of Kuromoto oscillators [9]. As shown in Fig. 1, within this smart power system model we incorporate PMUs, distributed control and distributed generation and storage. The use of such cyber components results in an overall system with both physical and cyber couplings such that when the physical system is incapable of achieving transient stability after a fault is cleared, the cyber couplings can provide enhancement through cyber-controlled power injection at the generator buses to encourage synchronization of the generator frequencies.

If the communications infrastructure is assumed to be lossless with delay τ, the overall cyber-physical dynamics for power flow can be described as follows [2]:

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

where $i = 1, \cdots, N$ is the agent's index, N is the number of agents, and the parameter $\alpha_i = 1$ for all i and the cyber-control signal is equal to $u_i = P_{u,i}$ (denoted $u_{i,\tau}$ in the presence of delay τ). To compute u_i to determine the degree of power injection/absorption at each generation bus, by the external fast-acting power source PMU data of every generator must be exchanged via a suitable communications network.

To reduce communication and control overhead, it was subsequently proposed by the authors that the natural under- or over-frequency clustering of generators after a fault could be leveraged to cluster the synchronous generators into high *physical* coherence groups. Assuming there are C clusters, the highest inertia generator of each cluster was then assigned as the corresponding "lead" generator. In the hierarchical formulation, the cyber-control is applied only to each of the C lead generators for transient stabilization of the lead generators while physical couplings are leveraged for stabilization of secondary generators. Thus, the overall dynamics of the system can be described by Eq. 1 above where

$$\alpha_i = \begin{cases} 1, & \text{if the } i\text{th agent is a lead agent;} \\ 0, & \text{otherwise,} \end{cases} . \tag{2}$$

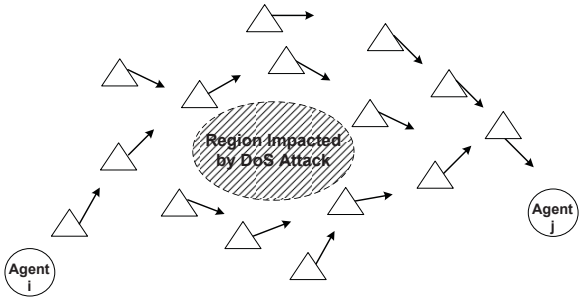

Fig. 3. The flocking behavior of network routing in the face of DoS attack.

We have shown that the communication delay τ must be "small" to meet the time requirements to guarantee transient stabilization [3]. Thus, one way in which an attacker could disrupt power system operation would be through DoS attacks on the communication system that would cause excessive latency or packet dropping. To characterize the effects of attacks an understanding of communications (via parameter τ) on transient stability (i.e., synchronization of Eq. 1) is needed.

III. Flocking-Based DoS-Attack-Resilient Routing Protocol

To better understand the interaction of communication network attacks on transient stability we aim to model the dynamics of communication network routing. Within this protocol, we denote a packet being processed and transmitted in the network as *active*. Packets with the same source-destination pair are said to comprise a *flock* with each member being a *flockmate*. Figure 3 illustrates a PMU data flock traveling hop-by-hop from Agent i to j while avoiding a region of DoS. Each network packet is considered to be generated at a given time index by its source and released into the network for propagation to its destination via interaction with the network infrastructure and other flockmates.

Large flocks in nature exhibit *behavioral transitions* such that future collective behavior is dependent on the previous history of individual orientation and group shape. Biologically this is important for the survival of animal groups to change from one type of structure to another in response to internal or external stimuli. We leverage this concept to model routing adaptation in the face of localized network attack. Our model of the network dynamics incorporates the states of both relay nodes and packets. We consider that each active packet communicates and interacts with its "predecessors". We define predecessors as neighboring flockmates generated at past time instants that are exactly one hop away or those flockmates that have just been transmitted from the relay nodes one hope away.

At the time step $t = k$, we define the state of the lth relay node as $\zeta_l = \{Q_{l,k}, \mathbf{R}_{l,k}\}$ where $Q_{l,k}$ is the queue length in the node and $\mathbf{R}_{l,k}$ denotes the vector whose ith element represents the number of remaining hops from this node to the ith agent. We describe the state (at $t = k$) of an active packet generated at $t = m$ that is transmitted from Agent i to Agent j to be $\chi_{ij}^m(k) = [q_c(k), p_c(k), T_c(k)]$ where q_c is the packet's location described by the number of remaining hops to reach Agent j, p_c is its "routing velocity", and T_c its hop count. Thus, a packet's routing dynamics are described as:

$$\begin{cases} q_c(k+1) = q_c(k) + p_c(k), \\ p_c(k) = u_c(k), \\ T_c(k+1) = T_c(k) + 1, \end{cases} \tag{3}$$

where $u_c(k)$ is the abstracted routing protocol strategy. Once a packet is dropped, it is no longer exhibits dynamics.

An active packet's objective to reach its destination of Agent j is analogous to *goal seeking*. In relation to our dynamics, it suggests a desired velocity of $p_c^* = -1$. Thus we model a successful routing strategy as one for which the packet will aim to reduce or maintain its hop count from its destination. As a result we define $u_c(k) \in \{-1, 0\}$ and require that the next hop is to a relay node fulfils $\mathbf{R}_{l,k+1}(j) \leq q_c(k)$; such nodes are called possible candidate "hosting nodes."

As illustrated in Fig. 3, we model the region impacted by DoS as an obstacle such that routing dynamics must exhibit *obstacle avoidance*. The network and packets exchange state information to communicate the existence of a DoS. Specifically, at $t = k$, a packet traversing from Agent i to j that jumps to a new hosting node l interacts with it as follows:

$$\begin{cases} \mathbf{R}_{l,k}(i) = T_c(k), \\ q_c(k) = \mathbf{R}_{l,k}(j). \end{cases} \tag{4}$$

If more than one packet is transmitted from Agent i to j at $t = k$ then the minimum $T_c(k)$ will be assigned to $\mathbf{R}_{l,k}(i)$. Equation (4) describes how the states of the relay nodes are leveraged such that packets that are traveling from source Agent j gain insight into the hop count experience of one another. Thus packets that have traversed through a region impacted by a DoS will have the opportunity to make this known to those potentially crossing it form the opposite direction. Moreover, in our model, neighboring flockmates interact such that a positive (negative) hop experience of a predecessor to a given node positively (negatively) influences the likelihood of a current packet being routed to that node. In particular, for packet route selection all possible candidate host nodes for the next hop are classified and prioritized as shown in Fig. 4 using information from predecessor packets.

To select the next hop, a packet first tries to select a candidate host from the highest priority class. If multiple relay nodes exist in this class, then a *collision avoidance* (here, "collision" = overflow) strategy is employed by considering the remaining buffer space of each candidate. At $t = k$, we compute the following measure of *collision* (overflow) likelihood for the relay node l:

$$\mathcal{M}_l = \frac{r_{a,k-1} + Q_{k-1} - r_{d,k-1}}{r_{a,k-1} + Q_{k-1}}, \tag{5}$$

where $r_{a,k-1}$ and $r_{d,k-1}$ are, respectively, the number of packets arriving at and leaving the relay node at time $t = k-1$, and Q_{k-1} is the queue length of the node at time $t = k-1$. Equation (5) indicates that a relay node with smaller $\mathcal{M}_l$ has lower possibility of overflow at $t = k$. We also measure the

.

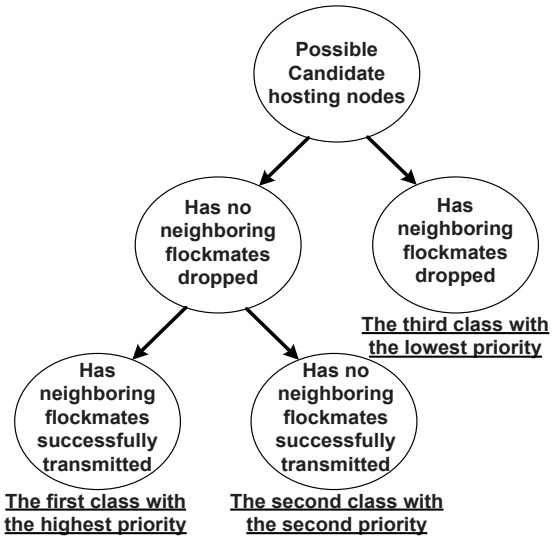

Fig. 4. Classification of the candidate hosting nodes.

alignment between the desired and actual velocity if the packet is transmitted to the relay node l as follows:

$$d_l = \begin{cases} 1, & \text{if } \mathbf{R}_{l,k}(i) < q_c(k), \\ \gamma, & \text{otherwise,} \end{cases} \tag{6}$$

where $\gamma > 1$ is a penalty parameter for not transmitting the packet closer to Agent j.

To balance the flocking principles of *goal seeking* (which promotes aggressive shortest-path routing to reduce latency) and *collision* (overflow) *avoidance*, we measure the desirability of a candidate host relay node as follows:

$$\mathcal{D}_l = \frac{1 - \mathcal{M}_l}{d_l}, \tag{7}$$

where the candidate with higher desirability $\mathcal{D}_l$ has higher likelihood of routing the packet. This is implemented by first ranking the candidate host nodes according to their $\mathcal{D}_l$ value. The probability of then routing to the nth node of the ranked list is given by $p_l = \beta(1-\beta)^{n-1}$ where the parameter $0.5 < \beta \leq 1$ controls the degree of randomization of our routing protocol; a smaller β indicates higher randomization and implies greater resilience to DoS while $\beta = 1$ represents aggressive shortest path routing with no randomization.

IV. Simulation

We demonstrate the performance of our proposed flocking-based hierarchical cyber-physical control framework with our DoS-attack-resilient routing protocol in maintaining transient stability on the 3-generator WECC system of Fig. 5. MATLAB/Simulink is employed for simulations. In order to demonstrate the utility of the proposed framework for wide area monitoring systems, the normalized impedance of the transmission line is increased from $0.1j$ (standard for the WECC system) to $0.35j$. The increase in impedance reduces the physical couplings amongst generators hence making the transient stability problem more challenging.

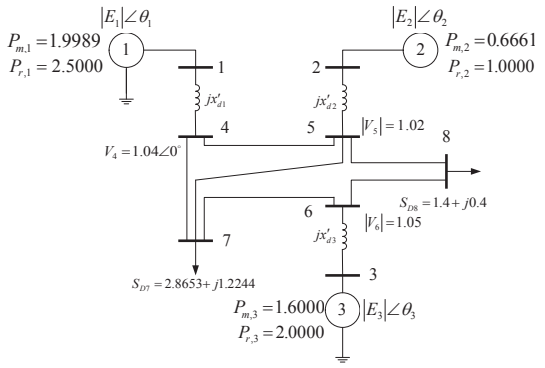

Fig. 5. WECC 3-generator power system

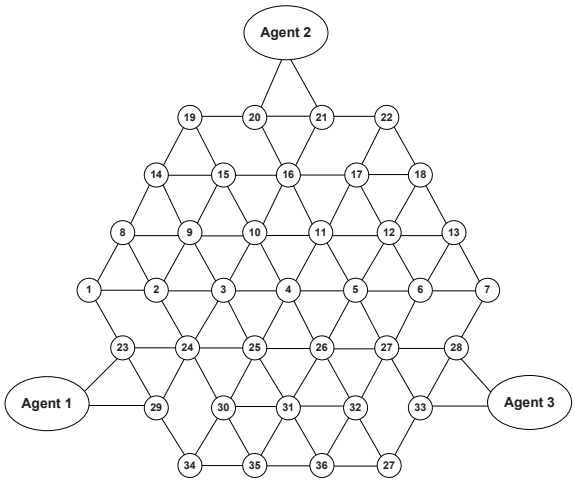

Fig. 6. The wide-area multi-hop network topology.

The mesh network of Fig. 6 used in our simulations has a uniform grid topology consisting of 37 relay nodes which are marked with their node indices. The buffer capacity of each relay node is set to 5, network link bandwith to 200 pkts/sec and the PMU sampling rate to 100 and 200 packets/sec for low and higher congestion scenarios, respectively.

We assume that a 3-phase short circuit fault occurs on the middle of Line $4-5$ of Fig. 5 at time $t = 0$ s and that the associated line is removed at $t = 0.3$ s, after the critical clearing time. The system behavior is shown in Fig. 7 over a period of 5 s and, as expected, the system loses stability; the normalized frequencies, phase angles and phase angle differences diverge beyond operating limits.

When our proposed flocking-based hierarchical control and communication framework is applied, we assume that cluster identification is achieved at $t = 0.35$ s and conclude that the physical system can be modeled as a dynamical system comprised of $\vartheta = 2$ clusters: $\{G_1\}$ and $\{G_2, G_3\}$ consistent with the results of Fig. 7. Figure 8 shows the hierarchy with Lead Agents 1 and 3. The cyber control is activated at $t = 0.4$ s which computes $u_i = P_{u,i}$ for each Lead Agent i.

The two routing control parameters γ designed to control "greediness" and β designed to control "randomization" of the protocol are varied. Figure 9 presents the routing packet delivery ratio for various selections of (γ, β) in the face of

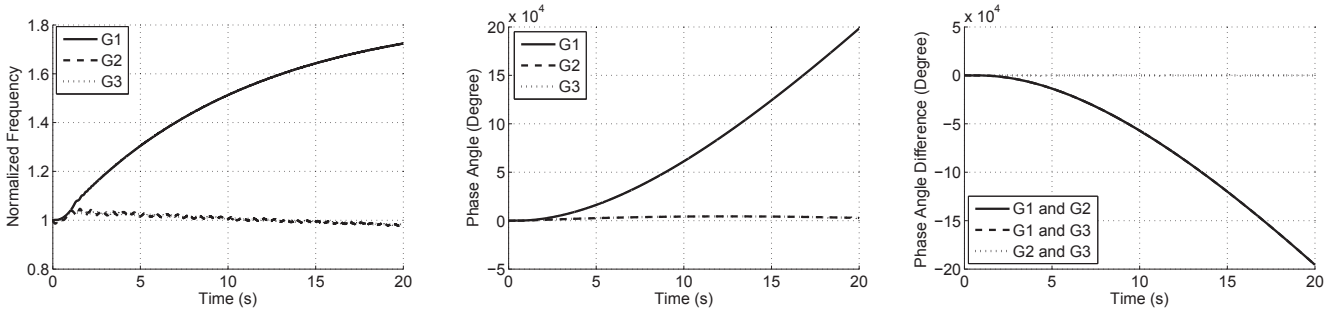

Fig. 7. Normalized rotor frequencies, phase angles, phase angle differences versus time without our proposed protocol.

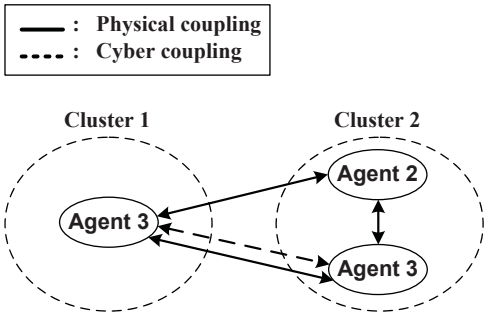

Fig. 8. Dynamical-graph representation of the physical system,

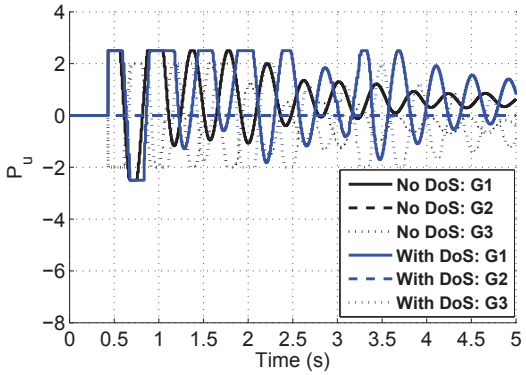

Fig. 12. Power injection/absorption P_u for flocking-based control in the absence and presence of DoS attack at Node 26 for $t \geq 2.5$ s. Clipping is evident given the maximum power constraints.

higher congestion and DoS attacks at Nodes 24 and 26 starting at time $t = 2.5$ s. As we observe, when no DoS is present lower randomization improves performance while penalty γ has negligible influence. In the face of DoS, effectively increasing β and selected γ can improve the networks resilience to attack. For instance, $(\gamma, \beta) = (3, 0.95)$ provides good performance for both DoS cases.

We next study the effect of the end-to-end delay of the network on the performance of transient stability mechanisms. Once again we focus on higher congestion and DoS attack on Nodes 24 and 26 at time $t \geq 2.5$ s. Parameter selections of $(\gamma, \beta) = (3, 1)$ and $(\gamma, \beta) = (3, 0.95)$ are made for the congestion and both DoS cases, respectively. Figure 10 demonstrates the performance of the routing protocol and its adaptation and resilience to DoS. For higher congestion, the routing strategy produces consistent latency since no randomization for routing ($\beta = 1$) is employed. However, in the face of DoS that is applied for $t \geq 2.5$ s, there is an adaptation stage at the beginning of communications for the flock in which experience is propagated amongst flockmates to improve performance. This occurs again amidst DoS. Overall, the adaptation enables good latency improvements within a few seconds.

Figure 11 evaluates the performance of our flocking-based hierarchical cyber-physical control framework in the presence of the proposed DoS-attack-resilient routing protocol for maintaining transient stability. We consider the network conditions of low congestion and DoS attack at Node 26 for $t \geq 2.5$ s with routing parameters $(\gamma, \beta) = (3, 1)$ and $(\gamma, \beta) = (3, 0.95)$, respectively. In both situations the PMU packet rate is set to 100 packets/sec. Moreover the power injection/absorption P_u from the fast reacting-source shown in Fig. 12 is constrained to be below the rated power in both cases [2]. It is clear from the generator performance that transient stability is maintained in the presence of series fault in the middle of Line $4 - 5$ and DoS attack thus demonstrating the potential of our cyber-physical modeling framework and proposed adaptive flocking-based routing strategy.

V. Conclusions

In this paper, we propose a flocking-based dynamical systems model for PMU communication routing in mesh networks for wide area monitoring. Such a model conveniently represents communication dynamics in a form that can be integrated with power system dynamics to provide a comprehensive framework for understanding cyber-physical system interactions. We demonstrate the utility of the model for demonstrating the advantages of employing flocking strategies for control and communications routing to maintain transient stability in the presence of severe physical power system fault and DoS attack on the network. Moreover we observe the advantages of *goal seeking* and *obstacle avoidance* strategies from flocking for timely and resilient data delivery.

VI. 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

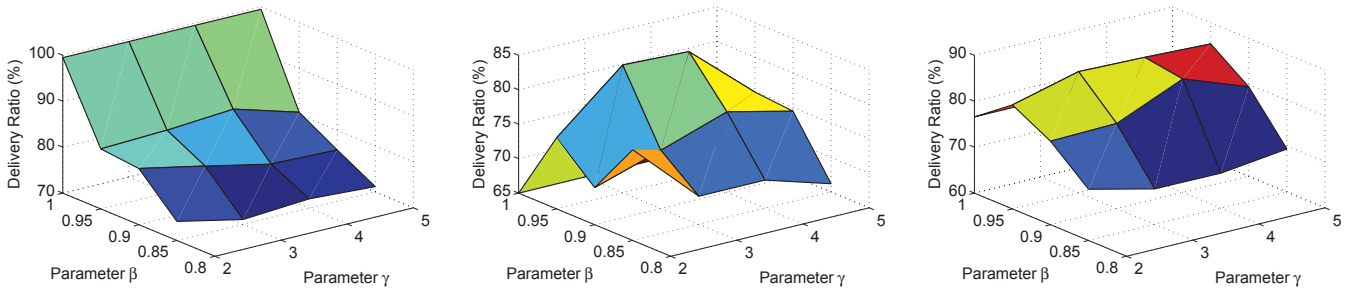

Fig. 9. Packet delivery ratio versus (γ, β) for 1) higher congestion, 2) DoS at Node 24 for $t \geq 2.5$ s, and 3) DoS at Node 26 for $t \geq 2.5$ s.

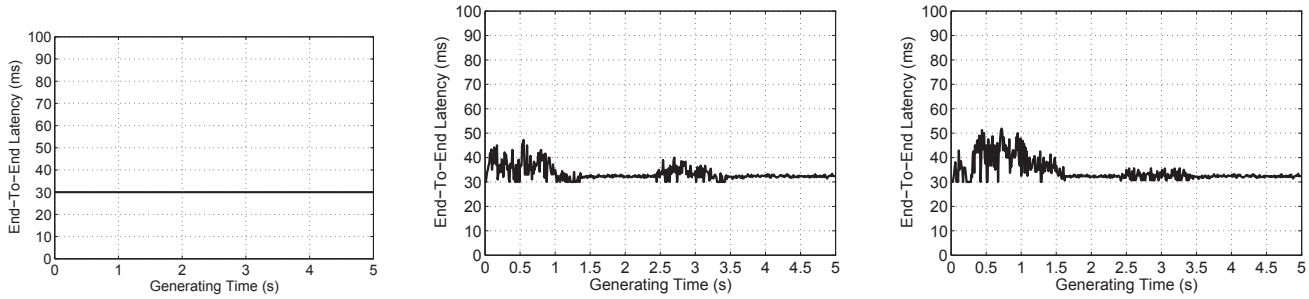

Fig. 10. End-to-End Latency versus packet generating time for 1) high congestion, 2) DoS at Node 24 for $t \geq 2.5$ s, and 3) DoS at Node 26 for $t \geq 2.5$ s.

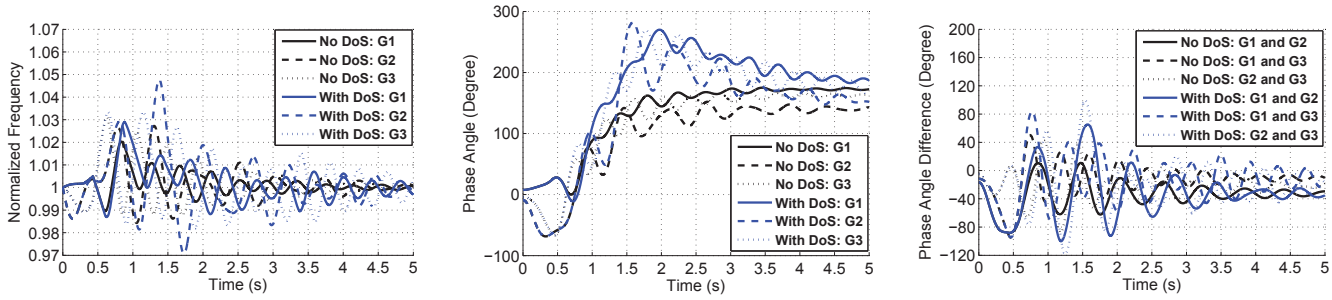

Fig. 11. Normalized rotor frequencies, phase angles, phase angle differences versus time with proposed cyber-physical control and routing protocol in the absence and presence of DoS attack at Node 26.

000512-0111-2009. The authors thank Xianyong Feng and Salman Mashayehk for stimulating discussions and comments during development of the work and Xianyong Feng for a preliminary version of the MATLAB simulation code.

REFERENCES

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

[2] 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 & Energy Society General Meeting*, San Diego, California, July 2012.

[3] J. Wei, D. Kundur, and T. Zourntos, "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, April-May 2012.

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

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

[6] D. Anderson, C. Zhao, C. Hauser, V. Venkatasubramanian, D. Bakken, and A. Bose, "A virtual smart grid: Real-time simulation for smart grid control and communications design," *IEEE Power and Energy Magazine*, vol. 10, no. 1, pp. 49–57, 2012.

[7] H. Gjermundrod, D. Bakken, C. Hauser, and A. Bose, "GridStat: A flexible qos-managed data dissemination framework for the power grid," *IEEE Transactions on Power Delivery*, vol. 24, no. 1, pp. 136–143, January 2009.

[8] N. Cherukuri and K. Nahrstedt, "Cooperative congestion control in power grid communication networks," in *Proc. International Conference on Smart Grid Communications (SmartGridComm)*, October 2011, pp. 587–592.

[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.