GOAliE: Goal-Seeking Obstacle and Collision Evasion for Resilient Multicast Routing in Smart Grid

Jin Wei and Deepa Kundur, *Fellow, IEEE*

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

***Index Terms*—Communications for wide-area monitoring, protection, and control (WAMPAC), cyber-physical flocking models, resilient multicast routing.**

I. Introduction

IT IS well known that the smart grid involves the integration of advanced measurement, communications, and control with the power delivery system. Phasor measurement units (PMUs) provide precise time-stamped voltage, current, and frequency information at acquisition rates ranging from 10 to 250 Hz at select locations of the grid [1]. The effectiveness of such high-fidelity data for grid monitoring and control is subject to communication timing guarantees [2]. As a result, the North American synchrophasor initiative (NASPI), a joint effort between the U.S. Department of Energy and the North American Electric Reliability Corporation, recently developed a reference communication infrastructure called NASPI network (NASPInet) to support PMU data delivery and specify recommended smart grid data delivery requirements including those related to latency and reliability [3], [4].

As one of the first and well-known standardized communication infrastructures for synchronous data delivery, NASPInet has been widely recognized as a guideline by other research association and companies for designing communication protocols and architectures. Since its proposal several communication networking research thrusts have focused on NASPInet requirements. Recently, Zhang *et al.* [5] proposed a centralized framework that optimizes the placement of trust nodes enabled with security services within the communication network and finds the least cost routing through such nodes. The approach has potential to achieve global efficiency and security, but its centralized structure limits scalability to large networks. In [6], a hybrid decentralized network architecture is proposed where routing decisions are based on dynamic network formation games to improve reliability. However, the efficiency of this unicast architecture is reduced for heavy traffic. Wei and Kundur [7] employed flocking principles to model smart grid information flow for routing over multihop mesh networks that accounts for latency and denial-of-service (DoS). Although the flocking paradigm has potential, the unicast nature of routing is performance-limiting for high traffic.

Recent studies have demonstrated the potential of multicast publish–subscribe network architectures to achieve the NASPInet requirements of low latency and high reliability [2], [8]. GridStat [9]–[11] is a quality of service (QoS)-managed network architecture based on a publish–subscribe paradigm. Here, the PMU data is delivered through a network of middleware-level status routers. Routing paths are determined by a hierarchical QoS management plane to achieve low latency and high reliability. Since routing computations are conducted offline, support currently does not exist to react to short-term changes in traffic. To address this issue, in [1] a cooperative congestion control (CCC) framework for real-time route determination in the GridStat is proposed. However, the authors only describe the general functions of CCC rather than provide implementation details. In [12], the frameworks of flocking and partial difference equation are proposed to study the communication infrastructure together with the power system stability. In [13], a flocking behavior-based unicast routing method is proposed for highly mobile ad hoc network. The overview of the routing method is introduced

Manuscript received December 27, 2013; revised July 7, 2014, December 3, 2014, and April 3, 2015; accepted May 20, 2015. Date of publication June 18, 2015; date of current version February 17, 2016. This work was supported in part by the U.S. National Science Foundation under Grant ECCS-1028246, in part by the Norman Hackerman Advanced Research Program under Project 000512-0111-2009, and in part by the University of Toronto. Paper no. TSG-00941-2013.

J. Wei is with the Department of Electrical and Computer Engineering, University of Akron, Akron, OH 44325 USA (e-mail: jwei1@uakron.edu).

D. Kundur is with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S3G4, Canada (e-mail: dkundur@comm.utoronto.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2015.2440184

without the model details. Furthermore, highly mobile ad hoc network, which this paper focuses on, is not appropriate for synchronous data delivery. In [14], a detailed multicast routing implementation is proposed for smart grid voltage control. Routing is formulated as an optimization problem assuming a simplified model of the physical system and heuristic solution approaches are applied. Questions arise as to its applicability to complex real-world smart grid topologies.

In this paper, we propose a flocking-based quality-of-experience (QoE)-managed multicast routing strategy, goal-seeking obstacle and collision evasion (GOAliE), based on a publish–subscribe paradigm. By predicting the impacted network region in real time and adaptively routing packets, this paper effectively mitigates the impact of the congestion and DoS attacks on the timely delivery of synchronous data that is critical for ensuring the appropriate smart grid operation and thus maintains the transient stability of power systems. Furthermore, in the GOAliE strategy, an intelligent multicast decision scheme is also developed, which dynamically manages the multicast packet replication process and efficiently balance the bandwidth (BW) consumption and end-to-end latency. The principles of this paper can be used in the existing standardized infrastructure such as Tropos mesh architecture proposed by ABB [15] and PMU network architecture proposed by CISCO [16]. Our flocking-based routing strategy is also expected to be integrated with our previous work on the flocking-based control strategy to achieve a cyber-physical dynamics in a higher-dimensional space to determine smart grid design strategies for overall system resilience to cyber and physical disruption. Compared with our previous work of unicast routing method in [7], the proposed strategy is developed based on a dynamic multicast decision scheme with efficient situational-awareness for network traffic. As stated in [15]–[22], the increasingly "meshed" power system topologies results in the requirement of the efficient, adaptive and flexible communication infrastructures, and the wide-area wired and wireless mesh networking solutions are emerging to meet this challenge. For example, the optical mesh networks, IEEE 802.16 WiMax mesh networks and IEEE 802.21 hybrid mesh networks are widely investigated with respect to smart grid applications. Therefore, in our framework, multicast routing protocol is implemented through a multihop mesh networking framework. We would like to clarify that our proposed multicast routing protocol is appropriate for both wired and wireless mesh networks. We focus on the development of a mathematical model to describe information flow that is compatible with existing models of power flows and does not require a simplification of physical system dynamics. To address the interaction between the physical system and routing protocol, we exploit the coupling between network packets carrying related measurement data to exchange valuable route experience information. Furthermore, our QoE-based multicast routing philosophy aims to be efficient and adaptive to unexpected traffic congestion and DoS.

The next section introduces our problem setting. Section III introduces our novel GOAliE paradigm for distributed dynamic multicast routing. Simulations and performance assessment for the well-known the New England 39-bus power system are provided in Section IV. The conclusion is given in Section V.

II. Problem Setting

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

A. Hierarchical Structure

The hierarchical structure applies to common distributed smart grid contexts. Here, agents with generators exhibiting high-physical coherence are said to form a cluster. Each cluster also consists of a phasor data concentrator as well as dedicated power or storage source(s) external to each agent often used for control. To reduce overhead, only one "lead" agent within the cluster is selected such that only it participates in cyber communication and control during operation, and its strong physical coupling to other agents' generators is exploited to regulate the overall cluster [23]. In this way, intercluster interactions are cyber-physical (tier-1) and intracluster synergies are physical (tier-2).

We illustrate our hierarchical communication framework for the well-known New England 39-bus system in Fig. 1(a). Here, we assume there are four clusters and the lead agent of each cluster is denoted with a shaded (green) generator. Effective PMU information (cyber) and power (physical) flows are presented as dashed and solid arrows, respectively. To further delineate the tiered nature of communications, red, blue, and magenta dashed arrows represent tiered communications from lowest to highest level.

The PMU information flows between lead agents are realized by the wide-area multihop mesh network of Fig. 1(b) successfully studied by a variety of authors for smart grid [1], [9], [24], [25]. The network consists of lead agents representing sources and sinks, relay nodes, and finite capacity communication links. To enable real-time guarantees in the face of network attack and congestion, we study a dynamic, distributed multicast routing protocol based on robust flocking principles.

B. Flocking for Routing

Flocking is a behavior exhibited by groups of birds participating in a shared objective that is difficult to achieve individually, but is possible through cooperation, consensus, and informed-adaptation. Members of a flock are referred to as flockmates or agents. Flocking behavior has been described by a set of heuristic agent-interaction rules [26], [27].

1) *Flock Centering:* Agents attempt to stay close to nearby flockmates.
2) *Velocity Matching:* Agents attempt to match velocity with nearby flockmates.

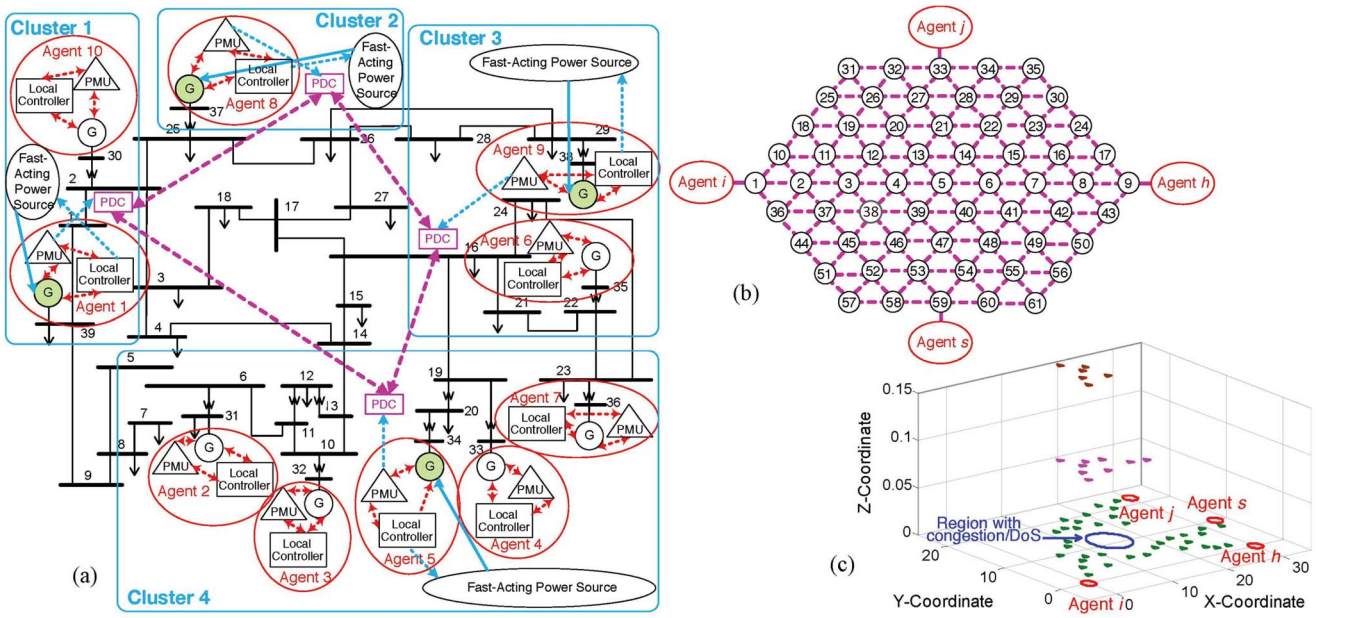

Fig. 1. (a) Hierarchical cyber-physical framework for the New England 39-bus power system. (b) Wide-area multihop mesh network. (c) Flocking-based paradigm for multicast network routing in the face of DoS attack.

3) *Goal Seeking:* Each agent has a desired velocity toward a specified position in global space.
4) *Obstacle Evasion:* Agents evade obstacles often steering away from their goals.
5) *Collision Avoidance:* Agents avoid collisions with nearby flockmates.
6) *Behavioral Transitions:* Past experience of the collective influences future behavior unbeknownst to individual flockmates.

Wei *et al*. [28] have formerly investigated the first three agent-interaction rules to reformulate the problem of transient stability in smart grid systems to one of flocking-based distributed multiagent control. Analogies of flock centering to generator phase angle cohesiveness, and velocity matching and goal seeking to exponential generator frequency synchronization were established requiring wide-area monitoring and communications be present.

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

In the next section, we demonstrate that successful principles for flocking provide valuable insight for the development of a resilient routing protocol for smart grid. We propose a novel approach for multiobjective dynamic multicast communications that is reactive to changing network environment to facilitate the need for resilience in smart grid. In multicast communication, the data sent from one node is copied and delivered to multiple destinations at different locations. Based on whether multicast groups are dynamic in nature, multicast routing methods can be classified into static multicast routing and dynamic multicast routing. In this paper, we focus on developing dynamic multicast routing approach, in which active multicast packets react to the changing network environment and dynamically determine when and how to be copied and sent to different destinations. We model multicast packet replication and route splitting as flock separation whereby a group of flockmates (collectively representing a multicast packet) experience forces of repulsion and attraction to one another based on routing objectives and network conditions. Finally, to promote self-healing networking, our routing paradigm employs experiential information from "predecessor" flockmates for adaptive congestion and DoS control.

III. Goal-Seeking Obstacle and Collision Evasion for Multicast Smart Grid Routing

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

Fig. 1(c) illustrates a PMU data flock traveling hop-by-hop from source agent i to destinations j, k, and l while avoiding a DoS region. We represent a single multicast packet intended for D destinations as D flockmates with identical (x, y) coordinates and distinct z-coordinates in the 3-D space as distinguished in Fig. 1(c) via hues of green, magenta, and brown stacked in the z-direction. To model multicast packet

replication and route separation, the corresponding flockmates would appropriately separate into two partitions in (x, y) space. The reader should note that within this framework unicast routing would reduce to 2-D flocking.

Network nodes are assumed to allow bidirectional multicast communications, be equipped with buffers, and be aware of their queue lengths, number of predecessors processed/dropped in the last ℓ time steps and an estimate of the minimum number of hops to a given destination. Under these assumption, by implementing our GOAliE routing method, the packets that have traveled through the region impacted by traffic congestion or DoS attacks have the opportunity to inform the packets that will potentially travel through the same region from the opposite direction, which realize the situational-awareness on the network changes and efficiently reduce the end-to-end latency caused by the traffic congestion or DoS attacks. As stated in [10] and [29], the processing delay is neglectable compared with the transmission delay for the application of synchronous data delivery, especially in the application with heavy traffic. Therefore, it is reasonable to assume that route decision-making does not cause significant processing delay.

We next discuss the details of GOAliE in two parts. Section III-A presents the selection of the next hop in multihop routing while Section III-B focuses on packet replication and route separation of multicast packets.

A. GOAliE Multihop Routing

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

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

$$p_c(k) = u_c(k) \text{ (update packet velocity for route decision)} \tag{1}$$

$$q_c(k+1) = q_c(k) + p_c(k) \text{ (update remaining hops)} \tag{2}$$

$$T_c(k+1) = T_c(k) + 1 \text{ (update total \# hops traversed)} \tag{3}$$

where $u_c(k)$ is the effect of the routing strategy measured in terms of the change in number of hops to the destination, which we assign to packet velocity $p_c(k)$. As illustrated in the following section, $u_c(k)$, which is achieved locally, reflects the varying network conditions. Equations (2) and (3) update the minimum number of hops to agent j and the running total of number of hops traversed, respectively.

1) Goal Seeking Constraint: We consider an analogy between an active packet's objective to reach its destination in a minimum number of hops and goal seeking. This suggests that an ideal goal for routing would be to have a packet velocity of $p_c^* = -1$, which implies that at each hop the packet is one hop closer to its destination. However, given the collaborative nature of our routing model, it is necessary to consider routing decisions that optimize other metrics such as the synchronization of other packets and buffer overflow. Furthermore, by considering that the situation is always time critical for transient stability maintenance, we design our routing strategy to prevent routing loop. Therefore, $u_c(k) = 1$ is not selected. Based on the above analysis, we permit our routing strategy to consider candidate next hop neighbors such that $u_c(k) \in \{-1, 0\}$.

2) Obstacle Evasion: As illustrated in Fig. 1(c), we model a region impacted by DoS or congestion as an obstacle that routing must circumvent. To facilitate informed obstacle evasion, the network nodes and packets exchange state information to communicate the existence of bottlenecks. At time k, a packet traversing from agents i to j that jumps to an intermediate node l interacts as follows:

$$\mathbf{R}_{l,k}(i) = T_c(k) \quad \text{packet} \xrightarrow{\text{state info}} \text{node} \tag{4}$$

$$q_c(k) = \mathbf{R}_{l,k}(j) \quad \text{node} \xrightarrow{\text{state info}} \text{packet}. \tag{5}$$

If more than one packet is traveling from source agent i at time k, then the minimum $T_c(k)$ will be assigned to $\mathbf{R}_{l,k}(i)$. Equation (4) allows node l to store the minimum hops traveled by packets from source agent i for later use by packets traveling to destination agent i assuming bidirectional symmetry. Conversely, in (5), node l updates the packet's hop distance to destination agent j using information it has previously acquired from agent j source packets. Therefore, for a given packet sent from agent i, the value of the minimum number of hops to its destination, agent j is expected based on the number of the experienced hops of the packet which is sent from agents j to i. By doing this, 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, so routing decisions may be made to evade the bottleneck.

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

4) Collision Avoidance: Flockmate collisions are employed as a metaphor for buffer overflow in a node. Let $\mathcal{M}_l$ be the collision (overflow) likelihood measure for a packet, traveling from agents i to j, on node l at time k. By considering the remaining buffer space of node l, we can conclude that: 1) the collision likelihood $\mathcal{M}_l$ is lower if the capacity of node l expected based on experience is higher and 2) $\mathcal{M}_l$ is higher if the remaining buffer space of node l predicted based on experience is higher. We achieve the following two formulas based on these two conclusion:

$$\begin{cases} \mathcal{M}_l \propto \dfrac{1}{\widetilde{r}_{a,k} + Q_l} \\ \mathcal{M}_l \propto \widetilde{r}_{a,k} + Q_l - \widetilde{r}_{d,k}. \end{cases} \tag{6}$$

Based on (6), we can develop the equation to predict the collision (overflow) likelihood $\mathcal{M}_l$ as follows:

$$\mathcal{M}_l = \frac{\widetilde{r}_{a,k} + Q_l - \widetilde{r}_{d,k}}{\widetilde{r}_{a,k} + Q_l} \tag{7}$$

where $\widetilde{r}_{a,k}$ and $\widetilde{r}_{d,k}$ are estimates of the number of packets arriving at and leaving the node l, respectively, for time k and Q_l is the queue length of node l at time $k-1$. Equation (7) indicates that at time k a node with smaller $\mathcal{M}_l$ has lower likelihood of overflow.

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

$$\begin{aligned} \widetilde{r}_{a,k} &= \sqrt{\frac{\sum_{n=1}^{\ell} h(n-1) r_a(n-1)^2}{\sum_{n=1}^{\ell} h(n-1)}} \\ \widetilde{r}_{d,k} &= \sqrt{\frac{\sum_{n=1}^{\ell} h(n-1) r_d(n-1)^2}{\sum_{n=1}^{\ell} h(n-1)}} \end{aligned} \tag{8}$$

where $r_a(\cdot)$ and $r_d(\cdot) \in \mathbb{Z}^+$ denotes, respectively, the number of arrivals and departures in the ℓ most recent time steps in chronological order, and $h(n)$ is the ℓ-point Hamming window $h(n) = 0.54 - 0.46\cos(2\pi n/2\ell - 3)$ giving highest weight to the most current information.

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

$$d_l = \begin{cases} 1, \text{ if } \mathbf{R}_{l,k}(i) < q_c(k) \\ \gamma, \text{ otherwise} \end{cases} \tag{9}$$

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

$$\mathcal{D}_l = \frac{1 - \mathcal{M}_l}{d_l} \tag{10}$$

where a candidate with higher desirability $\mathcal{D}_l$ has higher likelihood of routing the packet. Based on (7) and (8), the definition of the desirability $\mathcal{D}_l$ in (9) ensures that the candidate with less queue length, more successful data delivery experiences and less delivery failure has the higher desirability to be selected as the hosting node in the next time step. This is implemented by first ranking the candidate host nodes according to their $\mathcal{D}_l$ value. At each time step and for a packet v, a vector Υ_v is created whose elements are the indices of candidate hosts ordered in decreasing desirability. The probability of routing to the rth node of the ranked list is assigned geometrically with appropriate normalization factor $\overline{\beta}$ as follows:

$$p_r = \overline{\beta}(1-\beta)^r, \quad r = 1, 2, \ldots, |\Upsilon_v| \tag{11}$$

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 or sudden congestion while $\beta = 1$ represents aggressive routing with no randomization.

Thus, this section pertains to next hop selection for flockmates with different (x, y) coordinates. From (4)–(11), it is clear that the packet's decision of next hop selection is determined by the state information of the packet and that of the host node candidates. Since state information is updated locally, the next hop selection decision does not require global network information, which enables our scheme to be appropriate for large-scale networks. Flockmates with the same (x, y), but different z-coordinates (modeling a single multicast packet) must decide at each hop whether they must remain together or separate for multicast route splitting, as we discuss next.

B. GOALiE Multicast Routing

Multicast involves communications between a single source and multiple destinations such that a single packet is initially transmitted to save BW until it is decided that the packet must be replicated and split routes to balance individual destination latencies. In order to efficiently balance the BW consumption and the end-to-end latency, we develop an intelligent multicast packet replication management scheme. In this scheme, we address multicast routing through pairwise flockmate attraction and repulsion as a function of the congruence of their destinations.

Consider flockmates v and w with the same (x, y)-coordinates and distinct z-coordinates that represent components of a single multicast packet with different destinations. The multicast dynamics take place in the z-direction such that flockmates distant along z are considered to be repelled by one another and enable multicast splitting at the next hop. In contrast, flockmates in close proximity in z remain together for routing. We characterize the interaction at each time step k in terms of forces modeled via potential functions $V_1(k)$ and $V_2(k)$; the reader is referred to [30] for potential functions in the context of flocking. The associated acceleration between flockmates v and w is computed by differentiating the potential function with respect to the relative position vector between v and w in the z-direction.

Let Υ_{vw} be a vector of length L_{vw} consisting of elements in $\Upsilon_v \cap \Upsilon_w$ (representing candidate next hop hosts common to flockmates v and w). Each element of Υ_{vw} is associated with two routing likelihood values $\boldsymbol{v}_l = [p_{r_1}, p_{r_2}]$, $l = 1, 2, \ldots, L_{vw}$ [from (10) where r_1 and r_2 represent the rankings in order of decreasing desirability $\mathcal{D}_l$ of candidate host $\Upsilon_{vw}(l)$] for flockmates v and w, respectively. We let $\boldsymbol{v} = [\boldsymbol{v}_1 \ \boldsymbol{v}_2 \ \cdots \ \boldsymbol{v}_{L_{vw}}]$. A measure of congruency in the individual destination trajectories of flockmates v and w is evaluated as

$$\zeta_{vw} = \min\left\{\sum_{l=1}^{L_{vw}} \boldsymbol{v}_l(1), \sum_{l=1}^{L_{vw}} \boldsymbol{v}_l(2)\right\} \tag{12}$$

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

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

1) $\zeta_{vw} \geq \zeta_{th}$: We model the overall dynamics in the z-direction using the following potential energy function for time k:

$$V_1(k) = \sum_{v=1}^{L_{vw}} \sum_{w=1, w\neq v}^{L_{vw}} \frac{b_1}{b_2} \exp\big[b_2(\zeta_{vw} - \zeta_{\text{th}}) \big(\|z_v(k) - z_w(k)\|_\sigma - \|d^*\|_\sigma\big)\big] - b_1 \times (\zeta_{vw} - \zeta_{\text{th}})\big(\|z_v(k) - z_w(k)\|_\sigma - \|d^*\|_\sigma\big) \tag{13}$$

where $\|\cdot\|_\sigma$ denotes the σ-norm defined as: $\|\mathbf{x}\|_\sigma = (1/\epsilon)(\sqrt{1 + \epsilon\|\mathbf{x}\|} - 1)$, and ϵ, b_1, and b_2 are positive parameters. Equation (13) enables flockmate attraction without collision; a weak repulsive force is experienced when flockmate separation reaches d^*. The larger the value of $\zeta_{vw} - \zeta_{\text{th}}$, the stronger (weaker) the attraction (repulsion) force. The associated acceleration at time k is

$$g_{v,1}(k) = b_1 \sum_{w=1, w\neq v}^{L_{vw}} (\zeta_{vw} - \zeta_{\text{th}})\big\{\exp\big[b_2(\zeta_{vw} - \zeta_{\text{th}})(\|z_v(k) - z_w(k)\|_\sigma - \|d^*\|_\sigma)\big] - 1\big\}\mathbf{n}_{vw} \tag{14}$$

where $\mathbf{n}_{vw} = (z_w(k) - z_v(k)/\sqrt{1 + \epsilon\|z_w(k) - z_v(k)\|^2})$. Moreover, flockmates that belong to the same multicast group, interact to achieve velocity alignment. This is modeled as a distributed consensus problem [30] in which the flockmates are the vertices of a dynamic graph whose interaction to achieve alignment is determined by the graph's edge weight. The associated adjacency matrix elements are set to $a_{vw}(k) = 1$ if $\zeta_{vw} \geq \zeta_{\text{th}}$ and $a_{vw}(k) = 0$ otherwise. The corresponding acceleration is given by

$$g_{v,2}(k) = b_3 \sum_{w=1, w\neq v}^{L_{vw}} a_{vw}(k)(k)(\widehat{v}_v(k) - \widehat{v}_w(k)) \tag{15}$$

where $\widehat{v}_v(k)$ is flockmate velocity along the z-direction [see (18)].

2) $\zeta_{vw} < \zeta_{th}$: We consider the following potential energy function for repulsion:

$$V_2(k) = \sum_{v=1}^{L_{vw}} \sum_{w=1, w\neq v}^{L_{vw}} \frac{b_4}{2} a'_{vw}(k)(\zeta_{\text{th}} - \zeta_{vw}) (\|z_v(k) - z_w(k)\|_\sigma - \|d_r\|_\sigma)^2 \tag{16}$$

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

$$g_{v,3}(k) = b_4 a'_{vw}(\zeta_{\text{th}} - \zeta_{vw}) \sum_{w=1, w\neq v}^{L_{vw}} (\|z_v(k) - z_w(k)\|_\sigma - \|d_r\|_\sigma)\mathbf{n}_{vw}. \tag{17}$$

3) Multicast Dynamics and Decision-Making: The overall dynamics for the vth flockmate in the z-direction is

$$\begin{cases} \widehat{v}_v(k+1) = \widehat{v}_v(k) + \Delta t \sum_{l=1}^{3} g_{v,l}(k) \\ \widehat{z}_v(k+1) = \widehat{z}_v(k) + \Delta t \widehat{v}_v(k) \end{cases} \tag{18}$$

where Δt is the time between two consecutive time steps.

At each time step k, flockmates of the same multicast packet (from source agent i) cluster into $J_{n,i}$ subgroup(s) at a node n; a cluster algorithm such as [31] is used. If $J_{n,i} > 1$ let χ_m represent the set of common candidate hosts for flockmates in subgroup m and $\mathbf{W}_m$ be their set of destination agent indices. We assign the desirability for a candidate host l as $\widetilde{\mathcal{D}}_{m,l} = \max_{j\in\mathbf{W}_m}\{\mathbf{R}_{l,k}(j)\}$. We next rank the elements of χ_m in decreasing value of $\widetilde{\mathcal{D}}_l$ and assign a probability from (11) to obtain the expected remaining hops (for all subgroup flockmates to reach their destinations) if the group of packets is split into subgroups

$$\mathcal{R}_m = \sum_{r=1}^{\|\chi_m\|} p_r \widetilde{\mathcal{D}}_{m,r} \tag{19}$$

where r denotes the ranking of the candidate host node in χ_m.

Alternatively, we next assume no subgroup splitting and obtain the corresponding set $\widetilde{\chi}_i = \bigcap_{m=1}^{J_{n,i}} \chi_m$ consisting of the indices of common candidate hosts for all the members in the multicast group. Similarly, we define $\widehat{\mathcal{D}}_l = \max_{j\in\widehat{\mathbf{W}}}\{\mathbf{R}_{l,k}(j)\}$

where $\widehat{\mathbf{W}} = \bigcup_{m=1}^{J_{n,i}} \mathbf{W}_m$, and rank the elements in $\widetilde{\chi}_i$ in increasing value of $\widehat{\mathcal{D}}_l$. For each element of the reordered vector, we assign a probability from (11) and compute the expected number of minimum remaining hops assuming all flockmates stay in the same multicast group at time k

$$\widehat{\mathcal{R}} = \sum_{r=1}^{\|\widetilde{\chi}_i\|} p_r \widehat{\mathcal{D}}_r \tag{20}$$

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

At each time step, the splitting of flockmates within the same multipath group into $J_{n,i}$ subgroups may reduce end-to-end latency (or hop count), but will increase BW consumption by $(J_{n,i} - 1)$ units. We define the cost to reduce the BW as $f_b(n, i)$, which is positive, and define the cost to reduce the end-to-end latency as $f_l(n, i)$, which is negative

$$\begin{cases} f_b(n,i) = \max_{m=1}^{J_{n,i}} \{\mathcal{R}_m\} - \widehat{\mathcal{R}} \leq 0 \\ f_l(n,i) = \frac{J_{n,i}-1}{J_{n,i}} \geq 0. \end{cases} \tag{21}$$

Based on (21), we define the overall cost function $f(n, i)$ to balance these competing objectives, which is shown as follows:

$$f(n,i) = w_1 f_b(n,i) + (1 - w_1) f_l(n,i) \tag{22}$$

where parameter $w_1 \in [0, 1]$; here $w_1 = 0$ optimizes latency alone while $w_1 = 1$ solely considers BW consumption. Thus, at each time step, only if $f(n, i) < 0$, which means reducing the BW consumption costs more than reducing the end-to-end latency, the group of packets decides to split into $J_{n,i}$ subgroups. Otherwise they stay together. As soon as the subgroups separate, one packet in each subgroup normalizes its z-coordinate value to 0. The value of w_1 is numerically determined as shown in Section IV. The ongoing work focuses on the theoretical analysis of the optimal value of w_1.

IV. Simulations and Performance Assessment

Our simulations assess the performance of GOALiE using traditional communication performance metrics including packet delivery ratio and end-to-end latency. In addition, we evaluate GOALiE in the context of a critical smart grid distributed control application [28], maintaining transient stability in the face of fault(s) using wide-area PMU data. Such a setting illustrates the performance and resilience of routing when the need for data is most critical for power system operation. The performance of our multicast routing approach is compared to a unicast version formerly proposed by Wei and Kundur [7] and the multicast routing technique, multicast for *ad hoc* networks with swarm intelligence (MANSI), based on swarm intelligence [32]. Although MANSI is not designed specifically for smart grid communications routing, it aims for similar adaptive multicast characteristics as GOALiE providing an assessment of the advantage of using a flocking paradigm in particular.

We consider the New England 39-bus test power system of Fig. 1(a) as our underlying physical power system and employ the mesh network of Fig. 1(b) for communications; the mesh network has a uniform grid topology consisting of 61 nodes

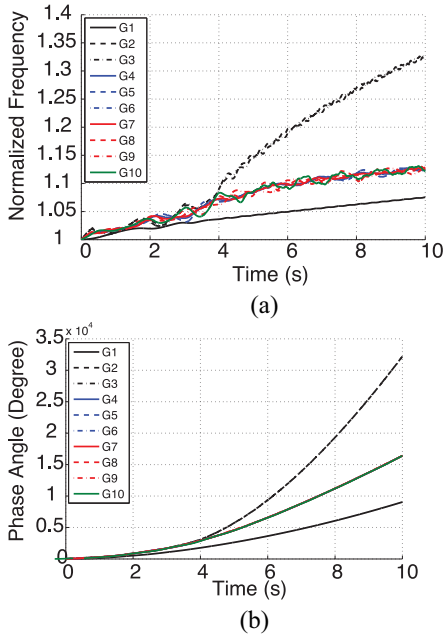

Fig. 2. (a) Normalized rotor frequencies. (b) Phase angles versus time without wide-area monitoring and control.

marked with their corresponding node indices in Fig. 1(b). Compared with building a dedicated network, in the practical implementation, it is more economically and technically efficient to achieve the synchronous data delivery by sharing with other applications in the existing network infrastructure. Therefore, in our simulation, we consider implementing our proposed GOALiE multicast routing method in a shared network. We set the buffer capacity of each node to be 5 and network link BW to 400 Kb/s for the application of synchronous data delivery. Furthermore, we set the PMU sampling rate to 100 and 200 packets/s for low and higher congestion scenarios, respectively. As suggested in [9]–[11] and [33], the PMU data packets are simulated by using C37.118 data frame with the packet size of 250 bytes. In addition, we assign parameters $\epsilon = 1$, $b_1 = 1$, $b_2 = 5$, $b_3 = 1/2$, $b_4 = 3$, and $\ell = 5$. To guarantee efficiency in maintaining the transient stability, we set the strict end-to-end deadlines to be 0.05 s. We assume in the face of a fault, the associated information needed to maintain transient stability has highest priority amongst all communication network information flows. MATLAB/Simulink is employed for simulations.

A. Case Study I

A three-phase short circuit fault occurs on the bus 14 of Fig. 1(a) at time $t = 0$ s. The associated lines 14 and 15 is removed at $t = 0.3$ s, post critical clearing time. The system behavior is illustrated in Fig. 2 over a period of 10 s and, as expected, stability is lost as the normalized frequencies, phase angles and phase angle differences diverge beyond operating limits.

When the distributed control approach of [28] is applied, post-fault clusters are first identified as $\{G_1\}$, $\{G_2, G_3\}$, $\{G_4, G_5, G_8, G_10\}$, and $\{G_6, G_7, G_9\}$ (at time $t = 0.35$ s) with lead agents selected as $i = 1, j = 3, h = 4$, and $s = 9$ that must

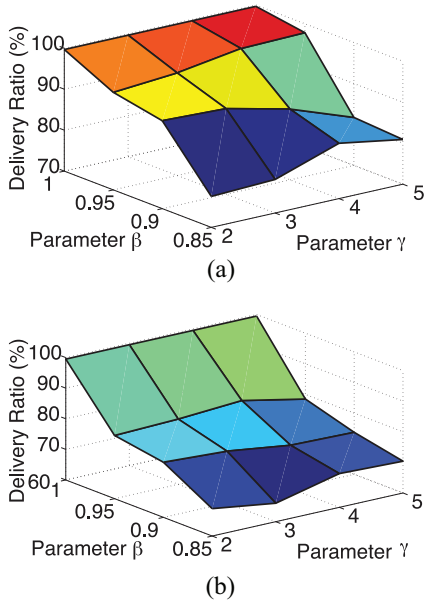

Fig. 3. GOAliE packet delivery ratio versus (γ, β) for (a) low congestion and (b) higher congestion.

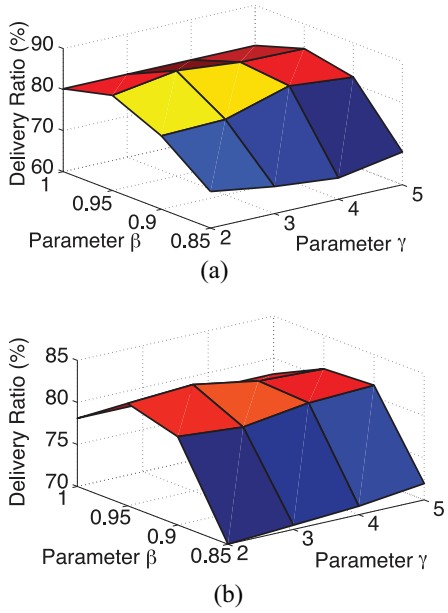

Fig. 4. GOAliE packet delivery ratio versus (γ, β) for (a) DoS attack at node 39 for $t \geq 5$ s and (b) DoS attack at nodes 5 and 6 for $t \geq 5$ s.

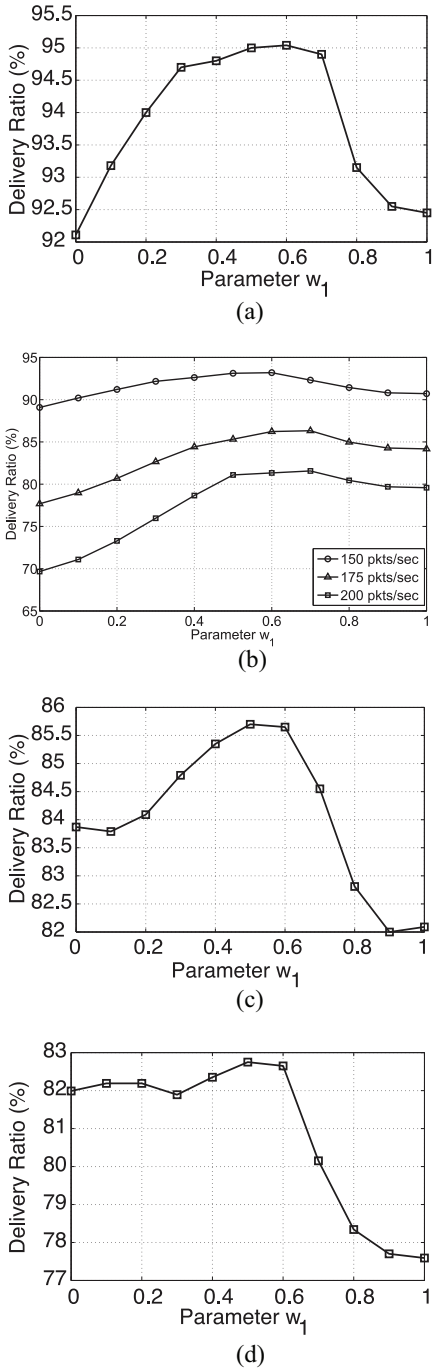

Fig. 5. GOAliE packet delivery ratio versus w_1 for (a) low congestion, (b) medium to high congestion, (c) DoS attack at node 39 for $t \geq 5$ s, and (d) DoS attack at nodes 5 and 6 for $t \geq 5$ s.

communicate through the network of Fig. 1(b). Cyber control is assumed to be activated at $t = 0.38$ s which requires real-time communications and control computation for each lead agent.

The GOAliE parameters γ designed to control "greediness" and β designed to control "randomization" of the multihop protocol are varied. Figs. 3 and 4 present the packet delivery ratio for varying of (γ, β).

Fig. 3 shows results for low and higher congestion, respectively, and Fig. 4 considers when congestion is low but DoS attacks are present starting at $t = 5$ s at node 39 and at nodes 5 and 6, respectively. In this paper, we model the DoS attack as: 1) if DoS attack occurs on a network link, the attacked link becomes unavailable and 2) if DoS attack occurs on a relay node, the attacked node and all the associated network links are unavailable. For all cases, we set $w_1 = 0.55$ (22). As observed, when no DoS is present lower randomization improves performance while 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.

For the same test conditions as Figs. 3 and 4 and for $(\gamma, \beta) = (3, 0.95)$, Fig. 5 presents the packet delivery

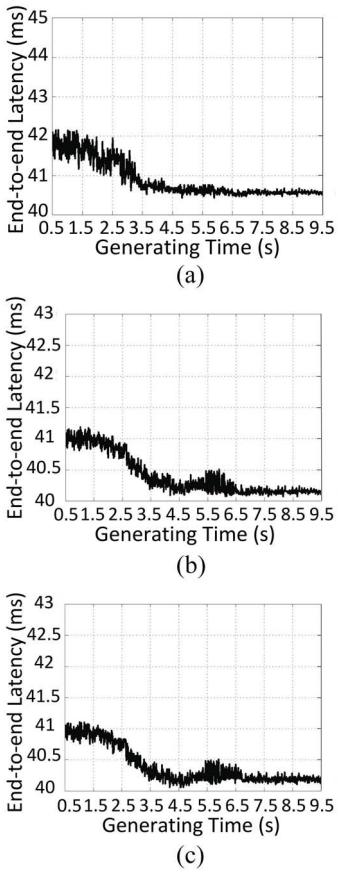

Fig. 6. GOAliE end-to-end latency versus packet generating time for (a) higher congestion, (b) DoS attack at node 39 for $t \geq 5$ s, and (c) DoS attack at nodes 5 and 6 for $t \geq 5$ s.

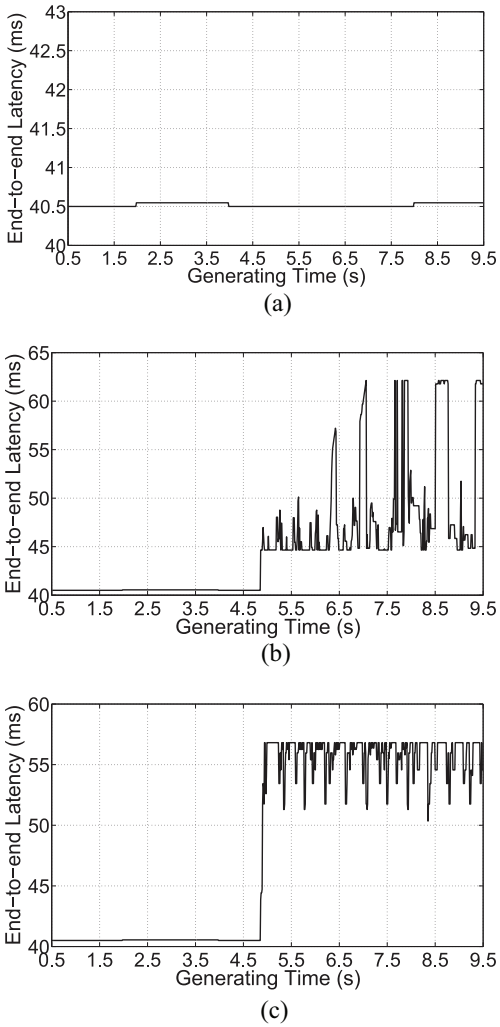

Fig. 7. End-to-end latency versus packet generating time by using dynamic DM multicast routing method for (a) higher congestion, (b) DoS attack at node 39 for $t \geq 5$ s, and (c) DoS attack at nodes 5 and 6 for $t \geq 5$ s.

ratio versus w_1. Fig. 5(a) considers the low congestion scenario in which PMU sampling rate is 100 packets/s. In Fig. 5(b), three different levels of network congestion are examined: 1) medium congestion with PMU sampling rate as 150 packets/s; 2) relatively higher congestion with PMU sampling rate as 175 packets/s; and 3) high congestion with PMU sampling rate as 200 packets/s. From Fig. 5(a) and (b), we can get that $w_1 \geq 0.5$ is needed in order to ensure resilience to the congestion. Furthermore, Fig. 5(c) and (d) shows the delivery ratio curves in the situation with DoS attacks. As observed, to ensure robustness to the DoS attack, $w_1 \leq 0.6$. Therefore, we set $w_1 = 0.55$ to address both classes of bottlenecks.

We next study end-to-end delay. Once again we focus on the situations of low and higher congestion and DoS attacks on node 39 ($t \geq 5$ s), and on nodes 5 and 6 ($t \geq 5$ s). Parameters are set to $(\gamma, \beta) = (3, 0.95)$ and $w_1 = 0.55$ for all cases. Fig. 6 illustrates the efficiency of our proposed GOAliE multicast routing strategy in reducing end-to-end latency in the presence of high congestion and DoS attacks. From Fig. 6, we can observe the natural adaptation stage at the beginning of communications in which experience is initially propagated amongst flockmates to improve performance and reduce end-to-end latency to a satisfactory value within 4.5 s. This also occurs amidst DoS attack to improve delay, which is demonstrated in Fig. 6(b) and (c). We can observe that the proposed routing strategy responds to the DoS attacks within 0.5 s, which is achieved through the exchange of flockmate experience. In order to compare the performance of our proposed GOAliE multicast approach with the classical dynamic multicast routing technique, we implement dynamic dense mode (DM) multicast routing method [34] under the same situations as Fig. 6 and evaluate the end-to-end latency in Fig. 7.

From Figs. 6 and 7, we can conclude that our proposed GOAliE multicast routing approach efficiently realizes the situational-awareness on the network changes and end-to-end latency reduction with the cost of increasing in the packet overhead to achieve dynamic multicast routing decision. Furthermore, in Table I, we also compare the performance between our proposed approach and the dynamic DM multicast approach in terms of the average throughput. From Table I, it is clear that, because of the procedure of propagating experience and the resulting packet overhead increase, the average throughput of our proposed method is slightly less than that of the dynamic DM multicast approach in the high-congestion situation. However, our proposed GOAliE method

TABLE I
COMPARISON RESULTS ON AVERAGE THROUGHPUT (Kb/s)

Multicast Routing Approaches	High Congestion	DoS Attack at Node 39	DoS Attack at Nodes 5 and 6
DM Multicast	112.16	99.01	99.31
GOAliE Multicast	112.03	111.03	111.71

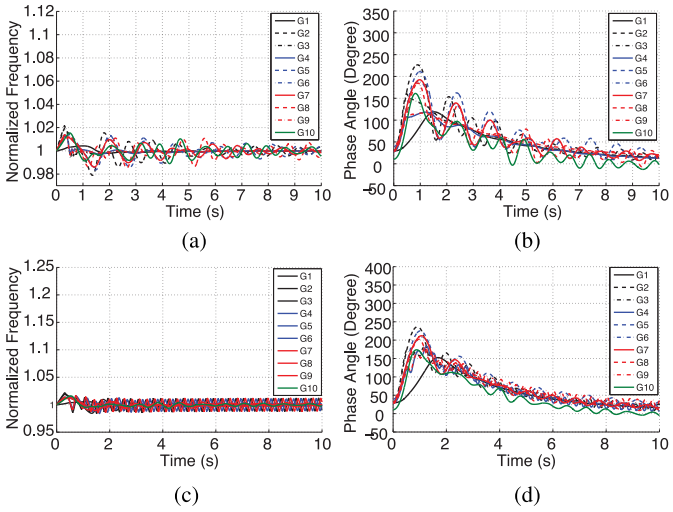

Fig. 8. Normalized rotor frequencies and phase angles versus time in the presence of distributed control [28] for high congestion: using (a) and (b) GOAliE and (c) and (d) unicast routing scheme [7].

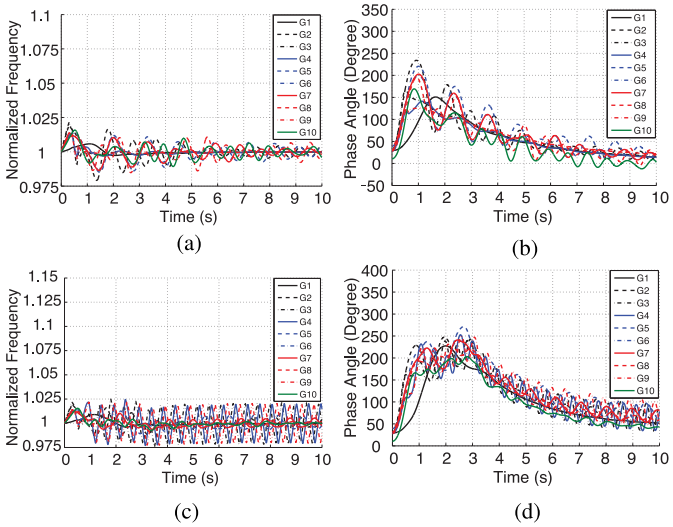

Fig. 9. Normalized rotor frequencies and phase angles versus time in the presence of distributed control [28] for DoS: using (a) and (b) GOAliE and (c) and (d) MANSI multicast routing [32].

notably outperforms the dynamic DM multicast method when there are unexpected DoS attacks.

Figs. 8 and 9 compare the performance of GOAliE with existing intelligent routing protocols [7], [32]. To assess performance in the context of a smart grid application, the effectiveness of the routing approach for wide-area communications for the distributed control scenario of [28] is considered. In Fig. 8, we consider high congestion and a PMU packet rate of 200 packets/s. We compare our proposed multicast routing scheme with the unicast version of [7] to observe that multicast routing efficiently improves

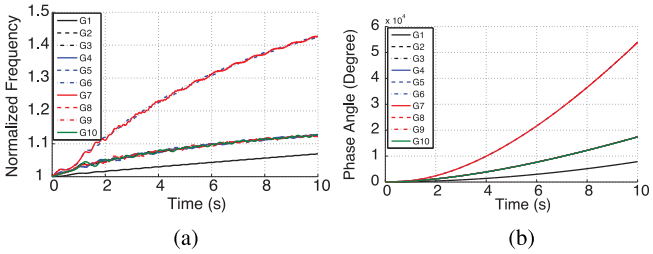

Fig. 10. (a) Normalized rotor frequencies. (b) Phase angles versus time without wide-area monitoring and control.

resilience to high congestion, which has a beneficial effect for real-time control as witnessed by the greater stabilization of frequency.

In Fig. 9, we consider DoS attack at nodes 5 and 6 for $t \geq 5$ s. The PMU packet rate is set to 100 packets/s for low congestion. We compare GOAliE to MANSI [32] and observed that our proposed approach is still more resilient to DoS attack by predicting the impacted network region in real time and adaptively routing packets. From Figs. 8 and 9, we can observe the effectiveness of our proposed routing strategy in mitigating the impact of congestion and DoS attacks on the in-time critical data delivery and ensuring transient stability maintenance for the power systems.

B. Case Study II

We assume that a three-phase short circuit fault occurs on the bus 21 of Fig. 1 at $t = 0$ s and that the associated lines 21 and 22 is removed at $t = 0.3$ s, post critical clearing time. The system behavior without control is shown in Fig. 10 over a period of 10 s and, as expected, stability is lost.

When the distributed control approach of [28] is applied, post fault clusters are identified as $\{G_1, G_{10}\}$, $\{G_2, G_3, G_4, G_5, G_8, G_9\}$, and $\{G_6, G_7\}$ at $t = 0.35$ with lead agents selected as $i = 1$, $j = 4$, and $h = 6$ that communicate through the multihop mesh network in Fig. 1(b) for real-time control beginning at $t = 0.38$ s.

Figs. 11 and 12 present the GOAliE routing packet delivery ratio for varying (γ, β) under low and higher congestion, and DoS attacks at node 21 and at nodes 27 and 28 both starting at $t = 5$ s. As observed, when DoS is not present lower degrees of randomization via parameter β improves performance while the penalty γ has negligible influence. For DoS, effectively increasing β and selecting 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 on the ability of distributed control to maintain transient stability. Once again we focus on higher congestion and DoS attacks on node 21 and on nodes 27 and 28 both for $t \geq 5$ s. Parameters were consistently set to $(\gamma, \beta) = (3, 0.95)$ and $w_1 = 0.55$. Fig. 13 demonstrates the successful performance of the routing protocol under both high congestion and DoS. From Fig. 13, we can see the routing experience is initially propagated amongst flockmates to improve the performance. Fig. 13(a) shows that, through the initial flockmate experience

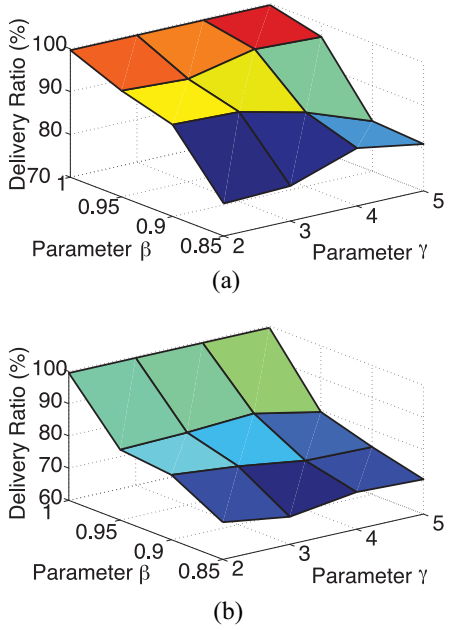

Fig. 11. GOAliE packet delivery ratio versus (γ, β) for (a) low congestion and (b) higher congestion.

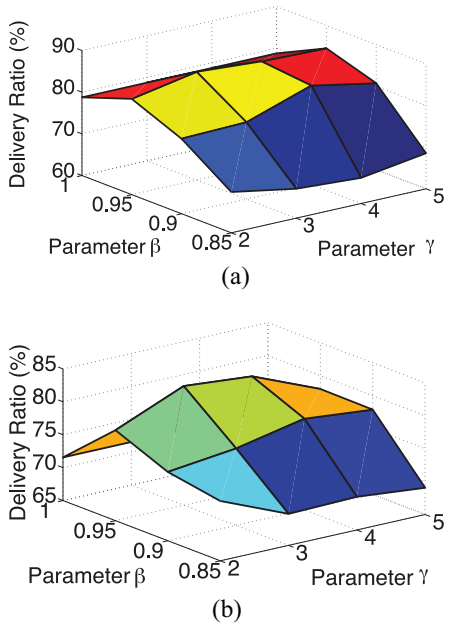

Fig. 12. GOAliE packet delivery ratio versus (γ, β) for (a) DoS attack at node 21 for $t \geq 5$ s and (b) DoS attack at nodes 27 and 28 for $t \geq 5$ s.

exchange, end-to-end latency is reduced to less than 40.5 ms within 4 s. Furthermore, Fig. 13(b) and (c) illustrates the self-healing property of our proposed routing strategy. We can observe that the proposed routing strategy responds to the DoS attacks within 0.5 s and adjusts the end-to-end latency back to less than 40.2 ms within 2 s.

Fig. 14 evaluates multicast routing performance for distributed control [28] of the New England 39-bus power system. We consider high congestion and DoS attack at nodes 5 and 6 for $t \geq 5$ s with parameters $(\gamma, \beta) = (3, 0.95)$ and $w_1 = 0.55$. The PMU packet rate is 200 packets/s for

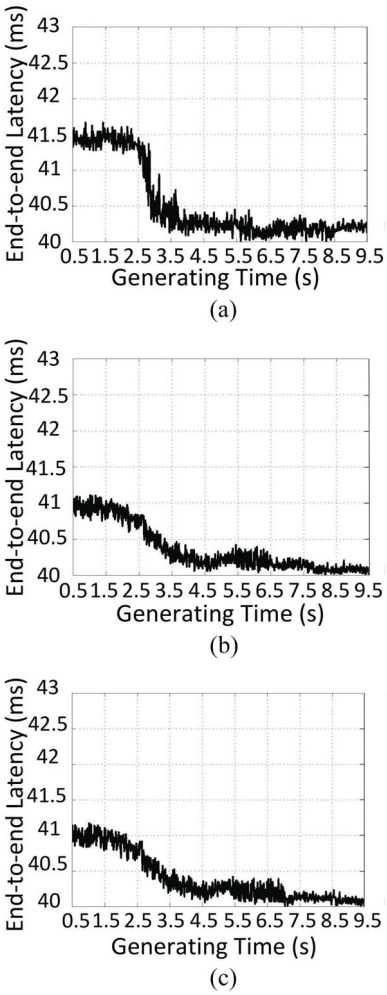

Fig. 13. GOAliE end-to-end latency versus packet generating time for (a) higher congestion, (b) DoS attack at node 21 for $t \geq 5$ s, and (c) DoS attack at nodes 27 and 28 for $t \geq 5$ s.

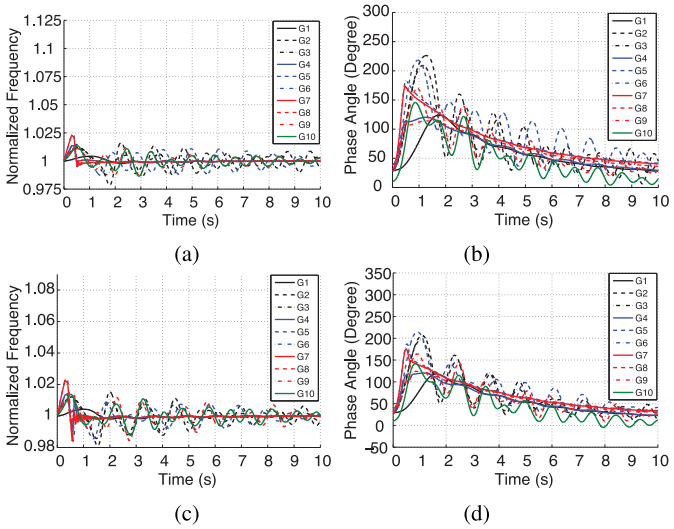

Fig. 14. Normalized rotor frequencies and phase angles versus time for distributed control [28]. For GOAliE (a) and (b) in the face of high congestion and (c) and (d) DoS attack.

high congestion and 100 packets/s for low congestion. It is clear from the generators' performance that transient stability is maintained in the presence of serious fault on the bus 21

through both high congestion, and DoS attack, thus demonstrating the potential of proposed adaptive multicast routing strategy.

V. Conclusion

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

We observe the advantages of goal seeking, obstacle evasion, collision avoidance, and behavioral transitions strategies from flocking for timely and resilient distributed multicast data delivery in comparison to existing routing techniques. We conclude that our distributed multicast routing approach, which that makes use of predecessor packet experiences much like flocks in nature, has the potential to facilitate an adaptive, self-healing, and resilient communications in smart grid applications. Our framework conveniently represents communication dynamics in a form that can be integrated with power system dynamics to provide a comprehensive framework for understanding cyber-physical system interactions. The ongoing work focuses on the theoretical analysis of the optimal value of w_1 which is the critical parameter to balance between the competing objectives of minimizing the end-to-end latency and BW consumption. For the future work, we will further analyze the tradeoff between robustness and low latency by allowing the packets to select a detour when there are DOS attacks or high congestion. We will also focus on integrating our proposed flocking-based GOAliE multicast routing method for the synchronous data delivery with our previous work on the flocking-based control strategy for the transient stability maintenance and achieving a cyber-physical dynamics in a higher-dimensional space to determine smart grid design strategies for overall system resilience to cyber and physical disruption.

References

[1] N. Cherukuri and K. Nahrstedt, "Cooperative congestion control in power grid communication networks," in *Proc. Int. Conf. Smart Grid Commun. (SmartGridComm)*, Brussels, Belgium, Oct. 2011, pp. 587–592.

[2] K. Kumar, M. Radhakrishnan, K. Sivalingam, D. Seetharam, and M. Karthick, "Comparison of publish–subscribe network architectures for smart grid wide area monitoring," in *Proc. Int. Conf. Smart Grid Commun. (SmartGridComm)*, Tainan, Taiwan, Nov. 2012, pp. 611–616.

[3] J. Dagle, "The North American synchrophasor initiative (NASPI)," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Calgary, AB, Canada, Jul. 2009, pp. 1–2.

[4] R. Bobba, E. Heine, H. Khurana, and T. Yardley, "Exploring a tiered architecture for NASPInet," in *Proc. IEEE PES Conf. Innov. Smart Grid Technol. (ISGT)*, Gaithersburg, MD, USA, Jan. 2010, pp. 1–8.

[5] Y. Zhang, L. Wang, and W. Sun, "Trust system design optimization in smart grid network infrastructure," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 184–195, Mar. 2013.

[6] Q. Zhu, D. Wei, and T. Basar, "Secure routing in smart grids," in *Proc. Workshop Found. Depend. Secure Cyber-Phys. Syst.*, Chicago, IL, USA, Apr. 2011, pp. 55–59.

[7] J. Wei and D. Kundur, "A flocking-based model for DoS-resilient communication routing in smart grid," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, Anaheim, CA, USA, Dec. 2012, pp. 3519–3524.

[8] D. Bakken, C. Hauser, and H. Gjermundrod, "Delivery requirements and implementation guidelines for the NASPInet data bus," in *Proc. Int. Conf. Smart Grid Commun. (SmartGridComm)*, Gaithersburg, MD, USA, Oct. 2010, pp. 37–42.

[9] H. Gjermundrod, D. Bakken, C. Hauser, and A. Bose, "GridStat: A flexible QoS-managed data dissemination framework for the power grid," *IEEE Trans. Power Del.*, vol. 24, no. 1, pp. 136–143, Jan. 2009.

[10] D. Bakken, A. Bose, C. Hauser, D. Whitehead, and G. Zweigle, "Smart generation and transmission with coherent real-time data," *Proc. IEEE*, vol. 99, no. 6, pp. 928–951, Jun. 2011.

[11] P. Kansal and A. Bose, "Bandwidth and latency requirements for smart transmission grid applications," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1344–1352, Sep. 2012.

[12] H. Li, S. Djouadi, and K. Tomsovic, "Flocking generators: A PDE framework for stability of smart grids with communications," in *Proc. IEEE 3rd Int. Conf. Smart Grid Commun. (SmartGridComm)*, Tainan, Taiwan, Nov. 2012, pp. 540–545.

[13] T. Srinivasan *et al.*, "BFBR: A novel bird flocking behavior based routing for highly mobile ad hoc networks," in *Proc. Int. Conf. Comput. Intell. Model. Control Autom. Int. Conf. Intell. Agents Web Technol. Internet Commer.*, Sydney, NSW, Australia, Nov./Dec. 2006, pp. 202–207.

[14] H. Li, L. Lai, and H. Poor, "Multicast routing for decentralized control of cyber physical systems with an application in smart grid," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 6, pp. 1097–1107, Jul. 2012.

[15] *Networking the Smart Grid*, ABB Tropos Wireless Commun. Syst., Sunnyvale, CA, USA, Sep. 2010.

[16] *PMU Networking With IP Multicast*, CISCO Syst., San Jose, CA, USA, 2012.

[17] *Communications Requirements of Smart Grid Technologies*, U.S. Dept. Energy, Washington, DC, USA, Oct. 2010.

[18] V. Pothamsetty and S. Malik, *Smart Grid: Leveraging Intelligent Communications to Transform the Power Infrastructure*, CISCO Syst., San Jose, CA, USA, Feb. 2009.

[19] E. Ancillotti, R. Bruno, and M. Conti, "The role of communication systems in smart grids: Architectures, technical solutions and research challenges," *Comput. Commun.*, vol. 36, nos. 17–18, p. 1665–1697, Nov. 2013.

[20] M. Daoud and X. Fernando, "On the communication requirements for the smart grid," *Energy Power Eng.*, vol. 3, no. 1, pp. 53–60, 2011.

[21] R. A. Schmidt, "Communications infrastructure for the smart grid," presented at the CRN Smart Grid Summit, Jun. 2010.

[22] J. Weikert, *DMS-Breakthrough Technology for the Smart Grid*, Power Syst. Eng., Madison, WI, USA, 2009.

[23] J. Wei and D. Kundur, "Two-tier hierarchical cyber-physical security analysis framework for smart grid," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, San Diego, CA, USA, Jul. 2012, pp. 1–5.

[24] P. Kulkarni, S. Gormus, Z. Fan, and F. Ramos, "AMI mesh networks: A practical solution and its performance evaluation," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1469–1481, Sep. 2012.

[25] D. Anderson *et al.*, "A virtual smart grid: Real-time simulation for smart grid control and communications design," *IEEE Power Energy Mag.*, vol. 10, no. 1, pp. 49–57, Jan./Feb. 2012.

[26] C. Reynolds, "Flocks, herds, and schools: A distributed behavioral model," *Comput. Graph.*, vol. 21, no. 4, pp. 25–34, Jul. 1987.

[27] I. Couzin, J. Krause, R. James, G. Ruxton, and N. Franks, "Collective memory and spatial sorting in animal groups," *J. Theoret. Biol.*, vol. 218, no. 1, pp. 1–11, 2002.

[28] 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 Soc. Gen. Meeting*, San Diego, CA, USA, Jul. 2012, pp. 1–8.

[29] B. Naduvathuparambil, M. Valenti, and A. Feliachi, "Communication delays in wide area measurement systems," in *Proc. 34th Southeast. Symp. Syst. Theory*, Huntsville, AL, USA, Mar. 2002, pp. 118–122.

[30] R. Olfati-Saber, "Flocking for multi-agent dynamic systems: Algorithms and theory," *IEEE Trans. Autom. Control*, vol. 51, no. 3, pp. 401–420, Mar. 2006.

[31] J. Wei and D. Kundur, "A multi-flock approach to rapid dynamic generator coherency identification," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Vancouver, BC, Canada, Jul. 2013, pp. 1–5.
[32] C. Shen and C. Jaikaeo, "Ad hoc multicast routing algorithm with swarm intelligence," *ACM Mobile Netw. Appl. J.*, vol. 10, nos. 1–2, pp. 47–59, 2005.
[33] R. Hasan, R. Bobba, and H. Khurana, "Analyzing NASPInet data flows," in *Proc. IEEE PES Power Syst. Conf. Exhibit. (PSCE)*, Seattle, WA, USA, Oct./Nov. 2006, pp. 1–6.
[34] L. Wei and D. Estrin, "Multicast routing in dense and sparse modes: Simulation study of tradeoffs and dynamics," in *Proc. 4th Int. Conf. Comput. Commun. Netw.*, Las Vegas, NV, USA, 1995, pp. 150–157.

Jin Wei received the B.E. degree in electronic information engineering from the Beijing University of Aeronautics and Astronautics, Beijing, China, in 2004; the M.S. degree in electrical engineering from the University of Hawaii at Manoa, Honolulu, HI, USA, in 2008; and the Ph.D. degree in electrical and computer engineering form the University of Toronto, Toronto, ON, Canada, in 2014.

She is an Assistant Professor of Electrical and Computer Engineering with the University of Akron, Akron, OH, USA. In 2014, she was a Postdoctoral Fellow with the National Renewable Energy Laboratory, Golden, CO, USA, for four months. Her current research interests include cyber-physical energy system, cyber-physical systems security, renewable energy integration, stochastic modeling and optimization of large-scale systems, and cognitive wired/wireless communication networks.

She was a recipient of travel grants and the IEEE Canadian Conference on Electrical and Computer Engineering'12 Best Student Paper Finalist.

Deepa Kundur (S'91–M'99–SM'03–F'15) received the B.A.Sc., M.A.Sc., and Ph.D. degrees from the University of Toronto, Toronto, ON, Canada, in 1993, 1995, and 1999, respectively, all in electrical and computer engineering.

She is a Professor of Electrical and Computer Engineering with the University of Toronto. Her current research interests include cyber security of the electric smart grid, cyber-physical system theory, security and privacy of sensor networks, and multimedia security and forensics.

Dr. Kundur was a recipient of the best paper recognitions at the 2008 IEEE INFOCOM Workshop on Mission Critical Networks, the 2011 Cyber Security and Information Intelligence Research Workshop, the 2012 IEEE Canadian Conference on Electrical and Computer Engineering, and the 2013 IEEE Power and Energy Society General Meeting. She currently serves as an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. She has served on the North American Reliability Corporation Smart Grid Task Force and has been on several editorial boards.