Resilient First-Order Consensus and Weakly Stable, Higher Order Synchronization of Continuous-Time Networked Multiagent Systems

Heath J. LeBlanc, *Member, IEEE*, and Xenofon Koutsoukos, *Senior Member, IEEE*

***Abstract*—Local interaction rules for consensus and synchronization are vital for many applications in distributed control of cyber-physical systems. However, most research in this area assumes all nodes (or agents) in the networked system cooperate. This paper considers local interaction rules for *resilient* first-order consensus and weakly stable, higher order synchronization whenever some of the agents in the network are Byzantine-like adversaries defined in a continuous-time setting. The normal agents have identical dynamics modeled by continuous-time, linear, time-invariant, weakly stable systems. Agents in the networked system influence one another by sharing state or output information according to a directed, time-varying graph. We present a resilient consensus protocol as well as dynamic state and output feedback control laws for the normal agents, to achieve the resilient consensus and synchronization objectives, respectively. We characterize the required network topologies using the property of network robustness. We demonstrate the results in simulation examples to illustrate the resilient synchronization output feedback control law.**

***Index Terms*—Adversary, Byzantine, consensus, distributed algorithms, resilience, robust networks, synchronization.**

I. Introduction

RECENTLY, local interaction rules have received great attention for application to distributed control of multiagent systems, and generally, cyber-physical systems (CPS). Many fundamental problems in distributed control of CPS can be reduced to an underlying consensus or synchronization framework, including formation control [1]–[3], distributed optimization [4], sensor fusion [5], distributed estimation [6]–[8], clock synchronization [9], and synchronization of the electric power grid [10], among others.

The consensus objective requires that the agents in the network achieve agreement on a certain state variable or set of state variables. Often agreement on the average, mean, or some other function of the state variables is desired [11]. First-order consensus involves integrator agents (in continuous-time setting), where convergence to a point in the state space is expected. Higher order consensus involves convergence to agreement of the state variables, which may be a specific point in the state space, or may be a time-varying trajectory [12], [13]. Often, convergence to a common, time-varying state trajectory is referred to as *synchronization* [14], which is the terminology adopted in this paper. A related problem to consensus in the literature is consensusability, which considers whether there exists a protocol that can achieve consensus given the dynamic model of the agent and the communication topology [15].

One of the major challenges in consensus or synchronization in networked multiagent systems is the hybrid dynamics that result from complex and dynamic interaction topologies (due to intermittent network link failures, mobility of the agents, or environmental factors). The continuous agent dynamics combined with the discrete dynamics of the switching network topologies results in a switched system.

Another major concern in networked multiagent systems is security. One approach to security is to improve the barriers to entry, such as the cryptographic techniques [16]. Another approach is to improve the resilience of the application layer protocols, such as the consensus and synchronization algorithms so that even in the event of an attack in which some nodes are compromised, the remaining uncompromised nodes (or normal nodes) are still able to achieve their objective (or perhaps a relaxed version of the objective).

A. Contributions

In this paper, we introduce a relaxed first-order consensus problem for the case when an unknown subset of nodes in the network are adversaries, which we call the resilient asymptotic consensus (RAC) problem for continuous-time agents. We describe a consensus protocol, referred to as the adversarial resilient consensus protocol (ARC-P) with parameter F. The focus on the consensus results of this paper is to characterize the structure of the network topology necessary and sufficient to achieve RAC in the presence of adversary agents.

The adversary agents considered in this paper are similar to Byzantine nodes, studied in fault-tolerant, distributed computing [17], which may behave arbitrarily within the confines of the model of computation. In the literature, it is commonly assumed

Manuscript received September 18, 2016; revised September 20, 2016 and March 7, 2017; accepted April 5, 2017. Date of publication April 24, 2017; date of current version September 17, 2018. This work was supported in part by the National Science Foundation (CNS- 1238959) and in part by the Air Force Research Laboratory (FA 8750-14-2-0180). Recommended by Associate Editor Prof. H. Ishii. *(Corresponding author: Heath J. LeBlanc.)*

H. J. LeBlanc is with the Electrical & Computer Engineering and Computer Science Department, Ohio Northern University, Ada, OH 45810 USA (e-mail: h-leblanc@onu.edu).

X. Koutsoukos is with the Department of Electrical Engineering and Computer Science, Vanderbilt University, Nashville, TN 37235 USA (e-mail: xenofon.koutsoukos@vanderbilt.edu)..

Digital Object Identifier 10.1109/TCNS.2017.2696364

2325-5870 © 2017 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

there are at most F Byzantine nodes in the network, which is an assumption we adopt. Each Byzantine node is allowed to be duplicitous, and can share different information with different neighboring nodes at a point in time (or round).

However, this assumption is not as reasonable in networked multiagent systems since often the network is based in wireless communication, where the channel is shared among the neighboring nodes. The "network" may also arise from measuring relative distances, such as in a robotic or vehicular network. Also, the models of computation of distributed computing are all discrete in nature; hence, time continuity is not a concern with Byzantine nodes.

In a continuous-time setting, with a switched system model, we must be concerned about continuity even for a well-formed solution. Any solution to a switched system without impulse effects has an absolutely continuous state trajectory [18], which is in turn uniformly continuous. The signals transmitted by agents in this paper are one or more of the following: 1) system states, 2) observer states, or 3) controller states. The model governing each of these quantities is a switched system without impulse effects, which is the model of computation inherited by the Byzantine-like adversary. Thus, in order to adapt the Byzantine node to the switched system model of the networked multiagent system, we assume the following: 1) all transmitted signals are uniformly continuous functions of time (including states, observer states, etc.),[1] 2) each adversary node conveys the same information to each out-neighbor in the network at any given point in time, and 3) there are at most F adversary nodes in the network.

A Byzantine-like attack model for a continuous-time setting is interesting and suitable for modeling attacks on CPS. CPS are characterized by complex dynamics, where the continuous dynamics are highly coupled and influenced by discrete factors, including the computation and communication approaches taken in the implementation. A node that is Byzantine, as we have outlined in continuous time, models nearly any type of attack on a node. Attacks on sensor or actuators will cause the node under attack to behave erratically, which is a special case of a Byzantine-like node. Similarly, a false data injection attack from the network would cause the node to make incorrect decisions, but still satisfy the assumptions of our model. However, it is important to emphasize that a node under attack is considered to be an adversary. Also, a Byzantine attack model does not capture attacks on the network itself, such as denial-of-service (DoS) attacks or jamming attacks.

We study resilient consensus in both time-invariant and time-varying networks. For time-invariant networks, we provide a necessary and sufficient condition on the network topology, based on the concept of network robustness [19], and show that RAC is achieved in the presence of the Byzantine-like adversary nodes. For time-varying networks, we require a uniform dwell-time assumption and provide a sufficient condition on the network robustness over time, asymptotically, in order to achieve RAC. This sufficient condition allows for the network to be poorly connected or even disconnected most of the time over any finite time interval, as long as it is sufficiently robust infinitely often, asymptotically.

The RAC problem studied here is a continuous-time analogue to the discrete-time RAC problem analyzed in [19]. Likewise, ARC-P with parameter F is the continuous-time analogue to the W-MSR algorithm studied in [19]. The contribution of the RAC results of this paper lie in the subtlety of analyzing a Byzantine-like adversary in a continuous-time setting, where the continuous variation of the trajectories in the worst case is more difficult than in discrete time where the trajectories are only defined at discrete instances of time.

In this paper, we also introduce a resilient asymptotic weakly stable synchronization (RAWSS) problem for the case when the normal agents are weakly stable, linear time-invariant (LTI) systems (meaning all eigenvalues are in the left-half plane and any eigenvalues on the imaginary axis must be nondefect). The goal is for each normal agent to asymptotically synchronize to a common, safe, and stable zero-input solution of the system despite the influence of adversary agents. Resilient synchronization controllers are designed for the case of full-state and output feedback. In the case of output feedback, a Luenberger observer is used to construct an estimate of the full state. The synchronization controllers make use of ARC-P as a consensus filter in such a way that the network topological conditions described in the resilient consensus results also apply to the RAWSS results. We provide a simulation example of a network of two-mass, two-spring systems under an actuator attack to illustrate the synchronization controllers.

B. Related Work

The research most closely related to this paper is the first-order resilient consensus results of [19]–[25], the second-order resilient consensus results of [26], and the synchronization results of [14] and [27]. In [19], [23], and [26], resilient consensus results are given under a discrete-time model. In [20]–[22], [24], and [25] resilient consensus results are given under a continuous-time model, similar to this paper; however, the sufficient condition on the time-varying network is much less general in [20]–[22] and [25] than Assumption 2 in this paper. Also, [25] assumes at most a specific fraction of neighboring nodes are adversary nodes, which requires a fractional notion of network robustness, and which has a significant gap between necessary and sufficient conditions on the time-invariant network consensus results. In [24], a resilient first-order consensus algorithm is analyzed in a time-invariant network under quantized communication. Resilient synchronization for more general LTI systems is not addressed in [19]–[25].

In [14], synchronization of identical linear systems is studied under similar assumptions on the normal agents described here. However, in [14], it is assumed that all agents cooperate in the synchronization process (i.e., all agents are normal). Here, we address resilient synchronization. Finally, the sufficient condition on the time-varying network in [27] is less general than Assumption 2. Specifically, in [27], it is required that each network at any point in time beyond a finite time t_0 must be

[1] Since continuous functions are uniformly continuous on any finite interval, this technical assumption is not practically much more restrictive than assuming pointwise continuity.

sufficiently robust, which is unrealistic in mobile ad hoc networks. Assumption 2 relaxes this requirement so that the network may even be disconnected much of the time.

The resilient synchronization control laws described here borrow ideas from [14]. The most important one is the reduction of synchronization to consensus by an appropriate change of variables involving the matrix exponential. The matrix exponential is used only in the analysis of the synchronization control laws of [14], whereas the matrix exponential is explicitly used in our control laws in order to decouple the modes of the LTI system before applying the piecewise linear resilient consensus filter ARC-P.

The research studying detection [28] and identification of malicious nodes [29]–[31] is related to this paper because similar adversary models are assumed. The approach in these works is to examine the behavior of nodes in the network to infer whether they must be misbehaving. Once isolated, the influence of the offending nodes may be removed. These approaches are computationally expensive and require special knowledge of the network topology in the algorithms. The detection technique of [28] is computationally efficient, but is not able to identify the misbehaving agents or reverse the negative effects caused.

There is a long history of research in resilient clock synchronization within the distributed computing literature [32], and progress is still being made [9]. Resilient consensus algorithms are often used in the process of clock synchronization, but the consensus process is on a set of logical clock values, which are decoupled from the underlying hardware that comprise the physical oscillators. The authors are unaware of any work on resilient synchronization of phase-locked loops, for example.

The rest of this paper is organized as follows. Section II defines the system model, the normal agent dynamics, the adversary model, and problem formulations. Section II-D describes the ARC-P with parameter F, which is used for the resilient consensus and synchronization results. Section II-F gives the definitions of network robustness needed for the main results. Section III provides the resilient consensus results and Section IV describes the resilient controllers and provides the analysis showing the resilience of the control laws to the influence of the adversaries. A simulation example is given in Section V to illustrate the utility of the synchronization controllers. Finally, Section VI concludes this paper.

II. System Model and Preliminaries

Consider a time-varying network modeled by the finite, simple directed graph (i.e., *digraph*) $\mathcal{D}(t) = (\mathcal{V}, \mathcal{E}(t))$, where $\mathcal{V} = \{1, ..., n\}$ is the *node (agent) set* and $\mathcal{E}(t) \subset \mathcal{V} \times \mathcal{V}$ is the *directed edge set* at time t. Without loss of generality, the node set is partitioned into a set of N *normal agents* $\mathcal{N} = \{1, 2, \dots, N\}$ and a set of M *adversary agents* $\mathcal{A} = \{N+1, N+2, \dots, n\}$, with $M = n - N \leq F$. It should be emphasized that this scheme for indexing is unknown to the normal agents; it is introduced for notational convenience. Each directed edge $(j, i) \in \mathcal{E}(t)$ indicates that node i can be influenced by node j at time t. In this case, we say that agent j *conveys* information to agent i. The sets of *in-neighbors* and *out-neighbors* of node i at time t are defined by $\mathcal{N}_i^{\text{in}}(t) = \{j \in \mathcal{V} : (j, i) \in \mathcal{E}(t)\}$ and $\mathcal{N}_i^{\text{out}}(t) = \{j \in \mathcal{V} : (i, j) \in \mathcal{E}(t)\}$, respectively, while the number of in-neighbors is given by the in-degree of node i at time t, $d_i(t) = |\mathcal{N}_i^{\text{in}}(t)|$. The set of all digraphs on n nodes is denoted by $\Gamma_n = \{\mathcal{D}_1, \dots, \mathcal{D}_d\}$.

The time-varying topology of the network is governed by a piecewise constant switching signal $\sigma : \mathbb{R}_{\geq 0} \to \{1, \dots, d\}$. At each point in time t, $\sigma(t)$ dictates the topology of the network, and σ is continuous from the right everywhere. In order to emphasize the role of the switching signal, we denote $\mathcal{D}_{\sigma(t)} = \mathcal{D}(t)$. Note that time-invariant networks are represented by simply dropping the dependence on time t.

A. Normal Agent Dynamics and Notation

The normal agents are assumed to be *identical*. Each normal agent $i \in \mathcal{N}$ has state $x_i \in \mathbb{R}^m$, control input $u_i \in \mathbb{R}^r$, and output $y_i \in \mathbb{R}^s$. The dynamics of each normal agent $i \in \mathcal{N}$ is given by the LTI system

$$\dot{x}_i = Ax_i + Bu_i \tag{1a}$$

$$y_i = Cx_i. \tag{1b}$$

The state $x_i(t) \in \mathbb{R}^m$ of normal agent $i \in \mathcal{N}$ at time t has components $x_{i,1}, x_{i,2}, \dots, x_{i,m}$. Similarly, its output $y_i(t) \in \mathbb{R}^s$ has components $y_{i,1}, y_{i,2}, \dots, y_{i,s}$. The components of the state and output of adversary agent $j \in \mathcal{A}$ are defined similarly.

B. Adversary Model

The adversary agents studied in this paper satisfy the following definition.

Definition 1 (F-Total Malicious Model): An agent $k \in \mathcal{A}$ is a *malicious adversary* (or just *malicious node*) if it is omniscient, and satisfies the following:

1) agent k conveys uniformly continuous signals to out-neighbors in the time interval over which the directed edge exists;
2) agent k conveys the same signals to all out-neighbors at any point in time;
3) there are at most F malicious adversaries in the network.

Other than these limitations, there are no further constraints placed on the adversary agents. Hence, this adversary model is similar to Byzantine nodes, which have been studied in distributed computing [17], [33], communication networks [34], [35], and mobile robotics [36]–[38].

C. Resilient Asymptotic Consensus Problem

The RAC problem is a continuous-time analogue to the *Byzantine approximate agreement problem* [17], [39]. Consensus—as studied here, in the RAC problem—requires agreement to a point in the state space. We focus on first-order consensus, where the agents have decoupled integrator dynamics. Hence, for consensus the LTI system model of (1) simplifies to $A = 0$ and $B = C = I$.

For the definition, we consider the intervals $\mathcal{I}_{t,k}$ defined by the kth component of the states of the normal nodes at time t as

follows. Let $\mathcal{I}_{t,k} = [m_{\mathcal{N},k}(t), M_{\mathcal{N},k}(t)]$, where

$$m_{\mathcal{N},k}(t) = \min_{i\in\mathcal{N}}\{x_{i,k}(t)\} \text{ and } M_{\mathcal{N},k}(t) = \max_{i\in\mathcal{N}}\{x_{i,k}(t)\}$$

are the minimum and maximum values, respectively, of the kth component of the states of the normal nodes at time t. Then, for each t we define the m-dimensional *orthotope* (or *hyperrectangle*) $\mathcal{H}_{t,\mathcal{N}}$ constructed from the intervals $\mathcal{I}_{t,k}$ by

$$\mathcal{H}_{t,\mathcal{N}} = \mathcal{I}_{t,1} \times \mathcal{I}_{t,2} \times \cdots \times \mathcal{I}_{t,m}.$$

Definition 2: The normal agents are said to achieve RAC in the presence of adversary agents (given a particular adversary model) if

1) $\exists L_k \in \mathbb{R}$ such that $\lim_{t\to\infty} x_{i,k}(t) = L_k$ for all $i \in \mathcal{N}, k = 1, 2, ..., m$;
2) $x_{i,k}(t) \in \mathcal{I}_{0,k} = [m_{\mathcal{N},k}(0), M_{\mathcal{N},k}(0)]$ $\forall t \in \mathbb{R}_{\geq 0}$, $i \in \mathcal{N}$, $k = 1, 2, ..., m$

for any choice of initial states $x_i(0) \in \mathbb{R}^m$, for $i \in \mathcal{N}$.

The RAC problem is defined by two conditions, agreement and safety, along with the type of adversary considered. Condition 1) in Definition 2 is an *agreement condition* that requires each of the states of the normal agents to converge to a common limit, despite the influence of the adversaries. It is important to explicitly require that the limit exists because in the terminology of this paper, consensus requires agreement on a specific value not changing with time. The safety condition in 2) is motivated by the validity condition of the Byzantine approximate agreement [17], [39]. The definition ensures that the values chosen by each normal agent lies within the range of "good" values. This is applicable in safety critical applications in which $\mathcal{H}_{0,\mathcal{N}}$ is a known safe set.

D. Resilient Consensus Algorithm

Since first-order consensus is applicable to normal agents with integrator dynamics (i.e., $A = 0$, $B = C = I$), we describe the ARC-P with parameter F for the case of scalar states $x_i(t) \in \mathbb{R}$. For vector states, simply apply the right-hand side of (2) to each component in the state vector. ARC-P simply sorts the values $x_j(t)$ from neighbors and removes up to F of the largest and smallest values from consideration. More precisely, if there are less than F values strictly larger than the normal node's own value, $x_i(t)$, then the node removes all of those values. Otherwise, it removes exactly the F largest values. Likewise, if there are less than F values strictly smaller than the normal nodes' own value, then it removes all of those values. Otherwise, it removes exactly the F smallest values. Let $\mathcal{R}_i(t)$ denote the set of neighbors whose values are removed by normal node i at time t. Then, ARC-P applied as the control input u_i of (1a) to a scalar integrator agent is given by

$$\dot{x}_i(t) = u_i = \sum_{j\in\mathcal{N}_i^{\text{in}}(t)\setminus\mathcal{R}_i(t)} w_{(j,i)}(t)\left(x_j(t) - x_i(t)\right) \qquad (2)$$

where the weights $w_{(j,i)}(t)$ are positive valued, piecewise continuous, and uniformly bounded (i.e., $0 < \alpha \leq w_{(j,i)}(t) \leq \beta$). A simple valid selection is to choose all weights to be one.

E. Resilient Asymptotic Weakly Stable Synchronization

Synchronization is similar to consensus in the sense that the states of the normal agents should asymptotically agree. However, synchronization does not require that the states of the agents be static in the absence of input. Hence, the notion of agreement for synchronization is defined in terms of convergence to a common zero-input trajectory of the LTI system model, rather than convergence to a common limit. We are specifically interested in both stable and safe zero-input trajectories, which leads to the definition of RAWSS.

Definition 3: Suppose the normal agents are identical LTI systems described by (1) and have initial states $x_i(0) \in \mathbb{R}^m$, for $i \in \mathcal{N}$. Let $\mathcal{S}_{0,\mathcal{N}} \subset \mathbb{R}^m$ be a safe set that contains the orthotope $\mathcal{H}_{0,\mathcal{N}}$; i.e., $\mathcal{H}_{0,\mathcal{N}} \subseteq \mathcal{S}_{0,\mathcal{N}}$. Then, the normal agents are said to achieve RAWSS in the presence of adversary agents (given a particular adversary model) if there exists a safe and stable, zero-input solution $x_0(t)$ that satisfies $\dot{x}_0(t) = Ax_0(t)$ for almost all $t \in \mathbb{R}_{\geq 0}$ with $x_0(0) \in \mathcal{S}_{0,\mathcal{N}}$, such that the normal states asymptotically converge to x_0; i.e.

$$\lim_{t\to\infty} ||x_i(t) - x_0(t)||_2 = 0 \ \ \forall i \in \mathcal{N}. \qquad (3)$$

A few remarks are in order with respect to the RAWSS problem. First, because the normal agents converge to a zero-input trajectory of the system, it is important that the system has no unstable modes. However, it is possible that the system matrix A is the result of local stabilization through an appropriate feedback controller so that the system in (1) is in fact a closed-loop feedback control system. Regardless of whether (1) defines the dynamics of a plant or a feedback control system, the control input u_i is viewed as the feedback control input from the multiagent network. Also, observe that the zero-input trajectory $x_0(t)$ to which the normal agents must converge satisfies the safety condition $x_0(0) \in \mathcal{S}_{0,\mathcal{N}}$. The safety condition requires that the adversary agents are not able to drive the normal agents to follow a zero-input trajectory with an unsafe initial state.

F. Network Robustness

Network robustness is a property of graphs formalizing the notion of sufficient redundancy of directed edges between subsets of nodes in the graph. For its definition, we require the following concept [19].

Definition 4 ((r,s)-Edge Reachable Set [19]): Given a nontrivial digraph $\mathcal{D}$ and a nonempty subset of nodes $\mathcal{S}$, we say that $\mathcal{S}$ is an (r,s)-*edge reachable set* if there are at least s nodes in $\mathcal{S}$ with at least r in-neighbors outside of $\mathcal{S}$, where $r, s \in \mathbb{Z}_{\geq 0}$; i.e., given $\mathcal{X}_{\mathcal{S}}^r = \{i \in \mathcal{S} : |\mathcal{N}_i^{\text{in}} \setminus \mathcal{S}| \geq r\}$, then $|\mathcal{X}_{\mathcal{S}}^r| \geq s$.

Edge reachability is used to define the global property of robustness, which essentially places lower bounds on the edge reachability properties of any pair of nonempty, disjoint subsets of nodes [19].

Definition 5 ((r,s)-robustness [19]): A nonempty, nontrivial digraph $\mathcal{D} = (\mathcal{V}, \mathcal{E})$ on n nodes ($n \geq 2$) is (r,s)-*robust*, for nonnegative integers $r \in \mathbb{Z}_{\geq 0}$, $1 \leq s \leq n$, if for every pair of nonempty, disjoint subsets $\mathcal{S}_1$ and $\mathcal{S}_2$ of $\mathcal{V}$ at least one of the following holds (recall $\mathcal{X}_{\mathcal{S}_k}^r = \{i \in \mathcal{S}_k : |\mathcal{N}_i^{\text{in}} \setminus \mathcal{S}_k| \geq r\}$ for $k \in \{1, 2\}$):

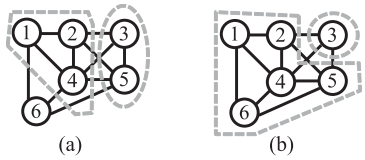

Fig. 1. Illustration of a (2, 3)-robust graph.

1) $|\mathcal{X}^r_{\mathcal{S}_1}| = |\mathcal{S}_1|$;
2) $|\mathcal{X}^r_{\mathcal{S}_2}| = |\mathcal{S}_2|$;
3) $|\mathcal{X}^r_{\mathcal{S}_1}| + |\mathcal{X}^r_{\mathcal{S}_2}| \geq s$.

By convention, if $\mathcal{D}$ is empty or trivial ($n \leq 1$), then $\mathcal{D}$ is (0, 1)-robust. If $\mathcal{D}$ is trivial, $\mathcal{D}$ is also (1, 1)-robust.

To illustrate network robustness, consider the (2, 3)-robust graph of Fig. 1. The main idea of (2, 3)-robustness is that between any two nonempty, disjoint pairs of subsets of nodes, there should be at least three nodes with at least two in-neighbors outside its set. This is captured by condition 3) of Definition 5 and illustrated by the choice of subsets shown in Fig. 1(a), where there are four (≥ 3) nodes in $\mathcal{S}_1 \cup \mathcal{S}_2$ with at least two in-neighbors outside their set (nodes 2–5).

However, it is possible to choose subsets for which the main idea of condition 3) cannot be true. For example, for the subsets of Fig. 1(b), there cannot be three nodes with at least two in-neighbors outside its set. Instead, all of the nodes in one of the sets has at least two in-neighbors from outside, which is illustrated by the singleton containing node 3 in Fig. 1(b), and captured in conditions 1) and 2) of Definition 5. Conditions 1) and 2) provide symmetry so that it does not matter which subset is labeled as $\mathcal{S}_1$ or $\mathcal{S}_2$.

Robust graphs tend to require high connectivity for large values of r and s; however for small values, the connectivity is not too large. For example, all digraphs with a rooted outbranching are (1,1)-robust. Also, proximity graphs will tend to be (2, 2)-robust as long as the spatial distribution of the nodes is not too great in comparison to the communication radius (and there are no isolated nodes). We note that the minimum in-degree of an $(F+1, F+1)$-robust digraph is $2F$. In [19], it is shown that the preferential attachment model of scale-free networks may be used to construct large robust networks from smaller ones. Moreover, in the limit of node size, robust networks share many qualities of random and complex networks [40].

G. Technical Assumptions

Several technical assumptions are given as follows that are used in the results of Sections III and IV.

Assumption 1: Each adversary state trajectory, $x_k(t)$ for $k \in \mathcal{A}$, must be uniformly continuous. Hence, for each $\nu > 0$, there exists $\delta_k(\nu) > 0$ such that $|x_k(t_1) - x_k(t_2)| < \nu$ whenever $|t_1 - t_2| < \delta_k(\nu)$. Define $\delta(\nu) = \min_{k\in\mathcal{A}}\{\delta_k(\nu)\}$.

Assumption 2: Given a time-varying network modeled by $\mathcal{D}_{\sigma(t)} = (\mathcal{V}, \mathcal{E}(t))$, let $\{t_j\}$ denote the switching times of $\sigma(t)$ and assume that $t_{j+1} - t_j \geq \tau$ for all j. Then, either 1) there exists an infinite subsequence of switching times $\{t'_j\} \subseteq \{t_j\}$ such that $\mathcal{D}_{\sigma(t'_j)}$ is $(F+1, F+1)$-robust, or 2) if $\exists t'_j$ such that $\mathcal{D}(t) = \mathcal{D}(t'_j)$ is $(F+1, F+1)$-robust $\forall t \geq t'_j$.

Assumption 3: System matrix A has all nondefect eigenvalues on the imaginary axis.

Assumption 4: The pair (A, B) is stabilizable.

Assumption 5: The pair (A, C) is detectable.

III. Resilient Consensus Analysis

In this section, we provide necessary and sufficient conditions under which ARC-P with parameter F achieves RAC under the F-total malicious adversary model. For first-order consensus, the LTI system model of (1) simplifies to $A = 0$, $B = I$, and $C = I$. Hence, we focus on the case with scalar state, with the understanding that ARC-P may be applied independently to each component and the results still hold. For the scalar case, we define

$$m_{\mathcal{N}}(t) = \min_{i\in\mathcal{N}}\{x_i(t)\} \text{ and } M_{\mathcal{N}}(t) = \max_{i\in\mathcal{N}}\{x_i(t)\}.$$

Lemma 1: Consider the normal agent $i \in \mathcal{N}$ using ARC-P with parameter F under the F-Total malicious model. Then, for each $t \in \mathbb{R}_{\geq 0}$

$$B(m_{\mathcal{N}}(t) - x_i(t)) \leq \sum_{j\in\mathcal{N}^{\text{in}}_i(t)\setminus\mathcal{R}_i(t)} w_{(j,i)}(t)\,(x_j(t) - x_i(t)) \leq B(M_{\mathcal{N}}(t) - x_i(t))$$

where $B = \beta(n - F - 1)$, which implies that $m_{\mathcal{N}}(t)$ and $M_{\mathcal{N}}(t)$ are monotonically nondecreasing and nonincreasing functions of time, respectively, and condition 2) of Definition 2 holds.

Lemma 1 shows that $M_{\mathcal{N}}(\cdot)$ is nonincreasing and $m_{\mathcal{N}}(\cdot)$ is nondecreasing, respectively, even in time-varying networks that may be disconnected much of the time. Therefore, if agreement is achieved among the normal agents, then the states of the normal agents must converge to a common limit. For this reason, we focus on proving that the Lyapunov candidate $\Psi(t) = M_{\mathcal{N}}(t) - m_{\mathcal{N}}(t)$ asymptotically vanishes (i.e., agreement is achieved).

In order to show that $\Psi(t)$ approaches zero asymptotically, we use a contradiction argument. Since $M_{\mathcal{N}}(\cdot)$ and $m_{\mathcal{N}}(\cdot)$ are monotonic and bounded, each has a limit, denoted by A_M and A_m, respectively. If $A_M = A_m$, then agreement is achieved (and thus, RAC). Initially, we focus on time-invariant networks and show that $(F+1, F+1)$-robustness is a necessary and sufficient condition for ARC-P with parameter F to achieve RAC under the F-total malicious adversary model. Network robustness guarantees a minimal amount of redundancy of incoming edges for each pair of nonempty, disjoint subsets of nodes $\mathcal{S}_1$ and $\mathcal{S}_2$ (c.f., Definition 5 and the example of Fig. 1). The sufficiency argument requires a judicious selection of nonempty, disjoint subsets such that the information from outside these subsets forces $\Psi(t)$ to shrink smaller than $A_M - A_m > 0$, which contradicts the assumption that $A_M - A_m > 0$ so that $A_M = A_m$.

The following lemma defines the subsets of nodes $\mathcal{X}_M$ and $\mathcal{X}_m$ that facilitate the sufficiency argument and it proves that these subsets are disjoint. The proof of the lemma requires the uniform continuity assumption of the F-total malicious model

(stated formally in Assumption 1) in order to ensure $\mathcal{X}_M$ and $\mathcal{X}_m$ are indeed disjoint. Otherwise, the adversaries can move from one set to the other, and we would not be able to choose a uniformly sized time interval to prevent that over the multiple time frames needed in the proof of Theorem 1.

Lemma 2: Consider a time-invariant network modeled by digraph $\mathcal{D}=(\mathcal{V},\mathcal{E})$ where the adversaries satisfy the F-total malicious adversary model. Suppose each normal node updates its value according to ARC-P with parameter F. For any $t_0 \geq 0$, $t \geq t_0$, $\Delta > 0$, and $\eta > 0$, define the sets of nodes

$$\mathcal{X}_M(t,t_0,\Delta,\eta)=\{i\in\mathcal{V} : \exists t'\in[t,t+\Delta] \text{ s.t. } x_i(t')>M_{\mathcal{N}}(t_0)-\eta\}$$
$$\mathcal{X}_m(t,t_0,\Delta,\eta)=\{i\in\mathcal{V} : \exists t'\in[t,t+\Delta] \text{ s.t. } x_i(t')<m_{\mathcal{N}}(t_0)+\eta\}.$$

If we select $\nu < (A_M - A_m)/2$ (from Assumption 1), $\Delta < \min\{\delta(\nu), \ln(3)/B\}$, and $\eta \leq (A_M - A_m)/4$, then $\mathcal{X}_M(t,t_0,\Delta,\eta) \cap \mathcal{X}_m(t,t_0,\Delta,\eta) = \emptyset$.

The necessary and sufficient condition on the network topology we consider in the following theorem is an $(F+1,F+1)$-robust graph. Lemma 2 used the uniform continuity assumption on the malicious agents' trajectories to ensure $\mathcal{X}_M$ and $\mathcal{X}_m$ are disjoint. In Theorem 1, we make use of this fact along with the assumption on the robust graph to show that our Lyapunov candidate must shrink beyond what would be allowed if convergence to consensus were not possible (i.e., a contradiction argument).

Theorem 1: Consider a time-invariant network modeled by digraph $\mathcal{D}=(\mathcal{V},\mathcal{E})$ where the adversaries satisfy the F-total malicious model. Suppose each normal node updates its value according to ARC-P with parameter F. Then, RAC is achieved if and only if the network topology is $(F+1,F+1)$-robust.

The sufficiency argument of Theorem 1 can be extended to time-varying networks under a uniform dwell-time assumption, as long as the network is $(F+1,F+1)$-robust infinitely often asymptotically. However, over any finite-time interval, the network need not be robust nor even be connected for most of the time. The assumption on the time-varying network needed for the result is formalized in Assumption 2.

Theorem 2: Consider a time-varying network, satisfying Assumption 2, where the adversaries satisfy the F-total malicious model. If each normal node updates its value according to ARC-P with parameter F, then RAC is achieved.

IV. Resilient Synchronization Analysis

In this section, we analyze control laws capable of achieving RAWSS under the F-total malicious adversary model. We first introduce a resilient synchronization controller for the case of full-state feedback. Then, we show how to extend the dynamic control law with output feedback using a Luenberger observer.

Each control law uses ARC-P with parameter F as a filter; thus, we need to introduce some notation to facilitate the description of the control laws. We represent the right-hand side of (2) in vector notation as

$$\Phi_F(\{x_j(t)\}_{j\in\mathcal{J}_i(t)}) = \begin{bmatrix} \sum_{j\in\mathcal{N}_i^{\text{in}}(t)\setminus\mathcal{R}_{i,1}(t)} w_{(j,i),1}(t)\,[x_{j,1}(t)-x_{i,1}(t)] \\ \vdots \\ \sum_{j\in\mathcal{N}_i^{\text{in}}(t)\setminus\mathcal{R}_{i,m}(t)} w_{(j,i),m}(t)[x_{j,m}(t)-x_{i,m}(t)] \end{bmatrix} \tag{4}$$

where $\mathcal{J}_i(t)=\mathcal{N}_i^{\text{in}}(t)\cup\{i\}$ is the set of inclusive in-neighbors of normal node i. In (4), the three steps of ARC-P with parameter F outlined in Section II-D are applied to each component k of the vectors independently. $\mathcal{R}_{i,k}(t)$ is the set of nodes whose kth component is removed by normal node i in Step 2 at time t. The weight functions are piecewise continuous and uniformly bounded by $0 \leq \alpha \leq w_{(j,i),k}(t) \leq \beta$.

For clarity, we present the RAWSS results in the two subsequent sections under the assumption that the system matrix A is nondefective with all eigenvalues on the imaginary axis.[2] If the system matrix has defective eigenvalues on the imaginary axis, then it is asymptotically unstable, which does not fulfill the requirement that the zero-input solution must always be stable. We may extend the analysis to the case where the system matrix has defective eigenvalues that are strictly stable, as these strictly stable modes trivially synchronize to zero without any control action. Throughout, it is assumed that the pair (A,B) is stabilizable and (A,C) is detectable, which are necessary conditions for consensusability of LTI agents [15]. It should be emphasized that all of the RAWSS results apply whenever Assumption 2 holds (i.e., if the network is sufficiently robust) since ARC-P is used as a filter in the control laws. Hence, the same sufficient condition on the time-varying network that was applied in the RAC results is applied to the RAWSS results.

A. RAWSS With Full-State Feedback

For RAWSS to be achieved, the normal nodes must synchronize to a common, stable zero-input solution of (1a), denoted $x_0(t)$, such that $x_0(0) \in \mathcal{S}_{0,\mathcal{N}}$. To do this, one term of the resilient control law first decouples the modes of the system matrix, and recovers the initial values of neighboring nodes in the decoupled coordinates using the associated matrix exponential. Then, the ARC-P consensus filter is used to effectively backtrack the initial values to consensus. Finally, the transformations are reversed.

The resilient control laws decouple the independent integrator modes (due to nondefect zero eigenvalues) from the independent oscillatory modes (due to conjugate pairs of nondefect imaginary eigenvalues) of nondefective system matrix A using an invertible linear transformation Q^{-1}, such that $A = QRQ^{-1}$, where R is given by

$$R=\begin{bmatrix} 0 & 0 \\ 0 & \text{diag}(R_2(\omega_1),\ldots,R_2(\omega_q)) \end{bmatrix}.$$

For concreteness, it is assumed that A has $p \geq 0$ nondefect zero eigenvalues and $2q$ nondefect nonzero eigenvalues on the

[2]Recall, the eigenvalues of a nondefective matrix have equivalent geometric and algebraic multiplicity, and nondefective matrices are diagonalizable [41].

imaginary axis. Each $R_2(\omega_l)$, for $l = 1, 2, \ldots, q$, is a 2×2 matrix of the form

$$R_2(\omega_l) \triangleq R_2(\lambda_{p+2l-1}, \lambda_{p+2l}) = \begin{bmatrix} 0 & -\omega_l \\ \omega_l & 0 \end{bmatrix}$$

where $\lambda_{p+2l-1} = -\omega_l \mathsf{i}$ and $\lambda_{p+2l} = \omega_l \mathsf{i}$, with $\omega_l \neq 0$ and $\mathsf{i} = \sqrt{-1}$. The matrix exponential of R is block diagonal and given by

$$e^{Rt} = \begin{bmatrix} I_p & 0 \\ 0 & \mathbf{diag}(e^{R_2(\omega_1)t}, \ldots, e^{R_2(\omega_q)t}) \end{bmatrix}$$

where I_p is the $p \times p$ identity matrix and

$$e^{R_2(\omega_l)t} = \begin{bmatrix} \cos(\omega_l t) & -\sin(\omega_l t) \\ \sin(\omega_l t) & \cos(\omega_l t) \end{bmatrix}.$$

The following lemma shows that if the input term Bu_i in (1a) is appropriately replaced, then RAWSS can be achieved. Throughout the rest of this paper, $||A||_2$ denotes the spectral norm of matrix A and $||x||_2$ is the two-norm of vector x [41].

Lemma 3: Suppose each agent $i \in \mathcal{N}$ is an LTI system as in (1), satisfying Assumption 3. Assume the time-varying network satisfies Assumption 2, and the adversaries satisfy the F-Total malicious model. Then, RAWSS is achieved if there exists a control law such that the closed-loop system for each normal node i is given by

$$\dot{x}_i(t) = Ax_i(t) + Qe^{\mathrm{R}t}\Phi_F\left(\{e^{-Rt}Q^{-1}x_j(t)\}_{j\in\mathcal{J}_i(t)}\right). \quad (5)$$

A dynamic, full-state, feedback controller that satisfies (5) in Lemma 3 can be designed for the case whenever (A, B) is stabilizable. Let K be a stabilizing gain matrix for the pair (A, B) and suppose the controller state η_i is initially relaxed (i.e., $\eta_i(0) = 0$ for all $i \in \mathcal{N}$). The dynamic control law is given by

$$\begin{aligned} \dot{\eta}_i &= (A + BK)\eta_i - Qe^{Rt}\Phi_F\left(\{e^{-Rt}Q^{-1}\xi_j(t)\}_{j\in\mathcal{J}_i(t)}\right) \\ u_i &= K\eta_i \end{aligned} \quad (6)$$

where $\xi_j(t) = x_j(t) - \eta_j(t)$, for $j \in \mathcal{V}$. Notice that either the ξ_j's alone are sent to out-neighbors or both x_j and η_j are sent in order to implement this control law. In either case, we require uniform continuity of the ξ_j, for $j \in \mathcal{A}$, which is captured in Definition 1.

Theorem 3: Suppose each agent $i \in \mathcal{N}$ is an LTI system as in (1) with full-state feedback (i.e., $C = I_m$), satisfying Assumptions 3 and 4, with stabilizing matrix K. Assume the time-varying network satisfies Assumption 2 and the adversaries satisfy the F-total malicious model. If each normal agent $i \in \mathcal{N}$ implements the dynamic control law in (6), then RAWSS is achieved.

B. RAWSS With Output Feedback

In this section, we study the case of output feedback whenever (A, C) is detectable (in addition to the previous assumptions). Here, we require a Luenberger observer in order to estimate the state. In this case, the dynamic control law is given by

$$\begin{aligned} \dot{\eta}_i &= (A + BK)\eta_i + H(\hat{y}_i - y_i) \\ &\quad - Qe^{Rt}\Phi_F\left(\{e^{-Rt}Q^{-1}\hat{\xi}_j(t)\}_{j\in\mathcal{J}_i(t)}\right) \\ u_i &= K\eta_i \end{aligned} \quad (7)$$

where $\hat{\xi}_j = \hat{x}_j - \eta_j$ for $j \in \mathcal{V}$. The observer is given by

$$\dot{\hat{x}}_i = A\hat{x}_i + Bu_i + H(\hat{y}_i - y_i) \quad (8a)$$

$$u_i = K\eta_i \quad (8b)$$

$$\hat{y}_i = C\hat{x}_i. \quad (8c)$$

Theorem 4: Suppose each agent $i \in \mathcal{N}$ is an LTI system as in (1) with output feedback, satisfying Assumptions 3–5, with stabilizing matrix K and observer matrix H. Assume the time-varying network satisfies Assumption 2 and the adversaries satisfy the F-Total malicious model. If each normal agent $i \in \mathcal{N}$ implements the dynamic control law in (7) with $\eta_i(0) = 0\,\forall i \in \mathcal{N}$ alongside observer (8) with observer states $\hat{x}_i$ for $i \in \mathcal{N}$ that are contained in some orthotope within the safe set $\mathcal{S}_{0,\mathcal{N}}$, then RAWSS is achieved.

Notice that the observer error term is used in the dynamic control law of (7) to ensure the form of (17) matches (5). The assumption that (A, C) is detectable guarantees that the observer error term vanishes asymptotically.

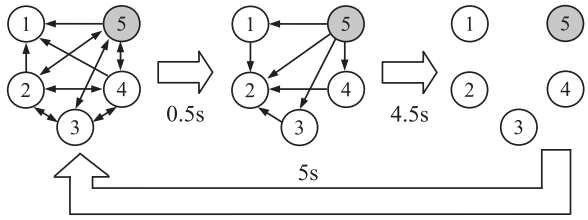

Fig. 2. Time-varying network of simulation scenario; node 5 is the adversary.

V. Simulations

In this section, we provide a numerical example to demonstrate the resilient output-feedback synchronization controller of (7). For this example, we consider a set of two-mass, two-spring coupled oscillators, each with masses $M_1 = 1$ kg and $M_2 = 2$ kg, and spring constants $k_1 = 1$ N/m and $k_2 = 0.5$ N/m. The input to each system (i.e., agent) is a force applied to mass M_2. This agent model is a fourth-order LTI system in which the first two states $x_{i,1}$ and $x_{i,2}$ denote the positions of the masses, while the second two states $x_{i,3}$ and $x_{i,4}$, denote their velocities. The state-space matrices are given by

$$A_i = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0.5 & 0 & 0 \\ 0.25 & -0.25 & 0 & 0 \end{bmatrix}, B_i = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0.25 \end{bmatrix}, C_i^{\mathsf{T}} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}.$$

Each agent has imaginary eigenvalues $\pm 0.3311\mathsf{i}$ and $\pm 1.0679\mathsf{i}$. We assume there are five such systems that share their position information according to the time-varying digraph depicted in

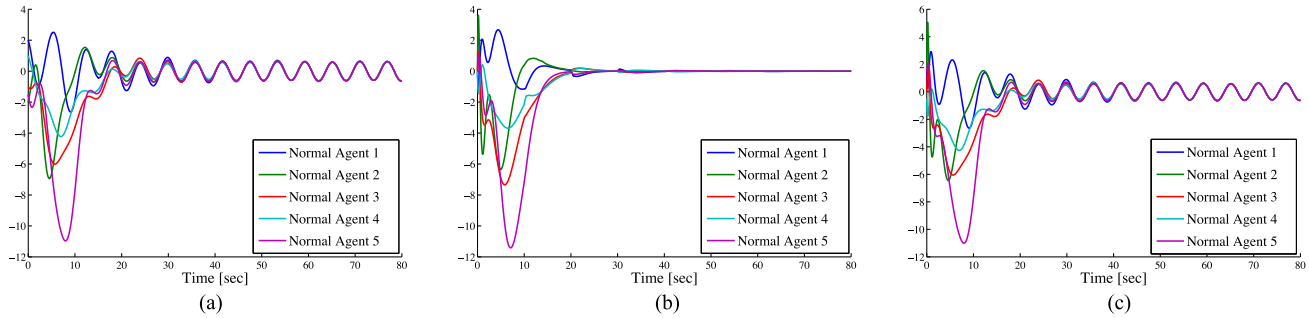

Fig. 3. Synchronization with no attack and $F = 1$. (a) First component of agent states. (b) First component of controller states. (c) First component of observer states.

Fig. 2. Observe that the first graph in the sequence is (2, 2)-robust, while the other two graphs are not. In fact, graph 3 has no edges at all. Out of every 10-s time interval, the network is given by the first graph for only 0.5 s, which is only 5% of the time.

Given the dynamic system model and time-varying network, we are interested in a control law on the force input that will synchronize the coupled oscillators to a common, safe, and stable zero-input trajectory of the system (i.e., achieve weakly stable synchronization). Moreover, we would like the synchronization to be resilient to an attack on one agent (the agent under attack becomes the adversary), even without detecting it. The control law of (7) will achieve this goal for any type of attack that may be modeled by the 1-total malicious model. We emphasize here that this adversary model is the most general attack model possible on a node, as it is unrestricted in how the attacked node behaves.[3] Hence, we may consider an attack on any one of the nodes, and may choose to attack the actuator, sensors, information received from or sent to the network, etc.

First, we consider the nominal behavior of the networked multiagent system whenever we have prepared for an attack on a node (i.e., chosen a parameter $F = 1$ for the ARC-P consensus filter), but there is no attack. Throughout the simulations, we use weights of 1 in ARC-P and the following parameters in the control law (7) and Luenberger observer (8):

$$Q = \begin{bmatrix} 0 & 0.9307 & 0 & -0.6574 \\ 0 & -0.2613 & 0 & -1.1706 \\ 0.9938 & 0 & -0.2176 & 0 \\ -0.279 & 0 & -0.3876 & 0 \end{bmatrix},$$

$$H = \begin{bmatrix} 8.75 \\ -15.75 \\ -17.375 \\ 0.875 \end{bmatrix}$$

$$K^{\mathsf{T}} = \begin{bmatrix} 22.75 \\ -12.75 \\ 8.75 \\ -14 \end{bmatrix}, e^{Rt} = \begin{bmatrix} e^{R_2(0.3311)t} & 0 \\ 0 & e^{R_2(1.0679)t} \end{bmatrix}.$$

[3]By assuming it is an attack on one of the agents, we are implicitly assuming the system model of (1), which admits uniformly continuous states and outputs. The network model assumes the same information propagates on all outgoing edges.

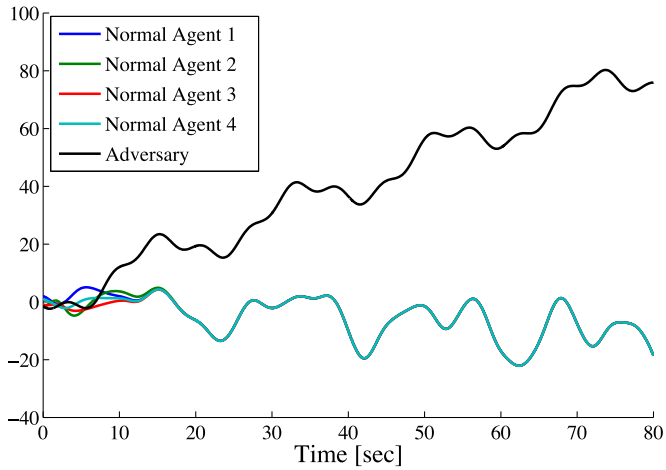

Fig. 4. First component of states with $F = 0$ and $u_5 = t$ (actuator attack).

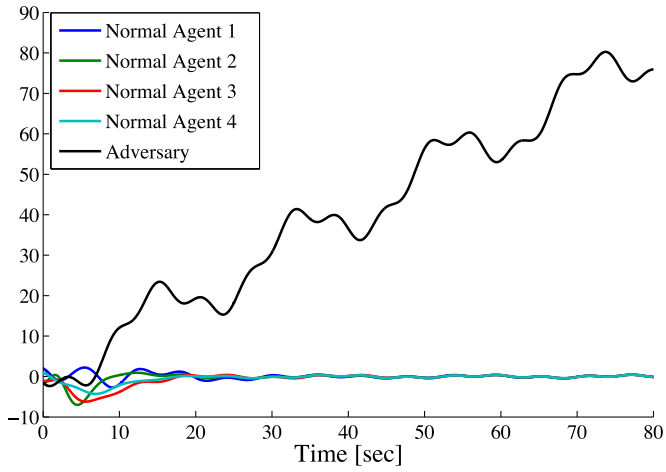

Fig. 5. First component of states with $F = 1$ and $u_5 = t$ (actuator attack).

The initial states of the agent systems and observers are randomly chosen within the interval $[-2, 2]$ for each component, which defines the orthotope $\mathcal{H}_{0,\mathcal{N}}$, given in the RAWSS definition (Definition 3). As required in Theorem 4, the controller states are set to zero. The results of the simulation with no attack and $F = 1$ is given in Fig. 3. Notice that the controller states

approach zero (and therefore, the control action goes to zero) as the agents synchronize.

Next, we demonstrate the need for the ARC-P consensus filter in the control law of (7). In this case, we prepare no resilience to an attack (i.e., the parameter $F = 0$), which leads to the dynamic synchronization control law of [14]. In this scenario, we assume the actuator of node 5 is attacked in such a way that $u_5 = t$. The results of this case are shown in Fig. 4. In this case, the normal agents still synchronize, but to an unsafe trajectory (initial state has components outside the interval $[-2, 2]$) that is clearly not a zero-state solution of the system.

Finally, we demonstrate the same actuator attack whenever the ARC-P consensus filter has parameter $F = 1$, which ensures resilience. The results of this case are shown in Fig. 5. In this case, the normal agents achieve RAWSS.

VI. Conclusion

This paper studies resilient consensus and synchronization of identical agents under a continuous-time LTI system model. A resilient consensus protocol, ARC-P with parameter F, is introduced, along with resilient control laws for synchronization. Necessary and sufficient conditions are provided under which the distributed control laws achieve their objective in both time-invariant and time-varying networks.

We emphasize that the parameter F of the consensus filter, ARC-P, should be selected at design time. The results of this paper provide guarantees on whether resilient consensus or weakly stable synchronization can be achieved in the presence of up to F malicious adversaries. The true number of adversaries is unknown to the designer at design time; hence, a reasonable value, typically small, should be chosen for parameter F since there is a tradeoff between resilience and the necessary robustness of the network.

Appendix

A. Proof of Lemma 1

Proof: If no neighboring states are used, or all states used are equal to $x_i(t)$ at time t, then $\dot{x}_i(t) = 0$, and the inequality holds. Therefore, assume $\exists j \in \mathcal{N}_i^{\text{in}}(t) \setminus \mathcal{R}_i(t)$ such that $x_j(t) \neq x_i(t)$. Then, $m_{\mathcal{N}}(t) \leq x_j(t) \leq M_{\mathcal{N}}(t)$; otherwise, j is an adversary and there are at least F more adversary state values in $\mathcal{R}_i(t)$. Hence, there are at least $F + 1$ adversary state values strictly greater than $M_{\mathcal{N}}(t)$ or strictly less than $m_{\mathcal{N}}(t)$ in the neighborhood, which contradicts the F-total assumption. Also, if $\exists j \in \mathcal{N}_i^{\text{in}}(t) \setminus \mathcal{R}_i(t)$ such that $x_j(t) \neq x_i(t)$, then there must be at least F state values in $\mathcal{R}_i(t)$. Since there are at most $n - 1$ neighbors of i, there are at most $n - F - 1$ nonzero terms in the sum of (2). Combining this with the fact that $w_{(j,i)}(t) \leq \beta$ for all $j \in \mathcal{N}_i^{\text{in}}(t)$ leads to the desired inequality.

Equation (3) defines the dynamics of the normal nodes. The inequality in the statement of the lemma ensures that if a normal node i has the largest state value at time t (i.e., $x_i(t) = M_{\mathcal{N}}(t)$), its derivative is nonpositive (meaning it will not increase) since the term $B(M_{\mathcal{N}}(t) - x_i(t)) = 0$ in this case. If a normal node has the smallest state value at time t (i.e., $x_i(t) = m_{\mathcal{N}}(t)$), its derivative is nonnegative (meaning it will not increase) since the term $B(m_{\mathcal{N}}(t) - x_i(t)) = 0$ in this case. Since $m_{\mathcal{N}}(t)$ and $M_{\mathcal{N}}(t)$ are continuous functions, they are monotonically nondecreasing and nonincreasing, respectively. Note that the monotonicity of $m_{\mathcal{N}}(t)$ and $M_{\mathcal{N}}(t)$ directly imply that condition 2) of Definition 2 holds. ■

B. Proof of Lemma 2

Proof: We consider separately the case for adversary nodes and normal nodes. Given the selection of η, ν, and Δ, the uniform continuity assumption prevents an adversary node from being in both sets. This follows because otherwise there exists $t_1, t_2 \in [t, t + \Delta]$ and $k \in \mathcal{A}$ such that $x_k(t_1) > M_{\mathcal{N}}(t_0) - \eta$ and $x_k(t_2) < m_{\mathcal{N}}(t_0) + \eta$, from which we reach the contradiction to uniform continuity

$$x_k(t_1) - x_k(t_2) > M_{\mathcal{N}}(t_0) - m_{\mathcal{N}}(t_0) - 2\eta \geq \frac{A_M - A_m}{2} > \nu.$$

For normal nodes, we first derive some useful inequalities. Applying Lemma 1 to (2) for $i \in \mathcal{N}$ and $\tau \in [t', t]$ implies

$$\dot{x}_i(\tau) \leq B(M_{\mathcal{N}}(\tau) - x_i(\tau)) \leq B(M_{\mathcal{N}}(t') - x_i(\tau))$$

whenever the derivative exists,[4] where $B = \beta(n - F - 1)$. Using the integrating factor $e^{B(\tau - t')}$, and integrating in the sense of Lebesgue over the time interval $[t', t]$, we have

$$x_i(t) \leq x_i(t')e^{-B(t-t')} + M_{\mathcal{N}}(t')(1 - e^{-B(t-t')}), \ \forall t \geq t'. \quad (9)$$

For $\tau \in [t, t']$, using integrating factor $e^{B(\tau - t)}$, we can show

$$x_i(t) \geq x_i(t')e^{B(t'-t)} + M_{\mathcal{N}}(t)(1 - e^{B(t'-t)}), \ \forall t \leq t'. \quad (10)$$

Similarly, we can derive the following inequalities using the other inequality of Lemma 1:

$$x_i(t) \geq x_i(t')e^{-B(t-t')} + m_{\mathcal{N}}(t')(1 - e^{-B(t-t')}), \ \forall t \geq t' \quad (11)$$

$$x_i(t) \leq x_i(t')e^{B(t'-t)} + m_{\mathcal{N}}(t)(1 - e^{B(t'-t)}), \ \forall t \leq t'. \quad (12)$$

Suppose $i \in \mathcal{N} \cap \mathcal{X}_M(t, t_0, \Delta, \eta)$. Then, $\exists t' \in [t, t + \Delta]$ such that $x_i(t') > M_{\mathcal{N}}(t_0) - \eta$. Combining this with (11), it follows that for $\tau \in [t', t + \Delta]$

$$\begin{aligned} x_i(\tau) &\geq x_i(t')e^{-B(\tau-t')} + m_{\mathcal{N}}(t')(1 - e^{-B(\tau-t')}) \\ &> (M_{\mathcal{N}}(t_0) - \eta)e^{-B(\tau-t')} + m_{\mathcal{N}}(t_0)(1 - e^{-B(\tau-t')}) \\ &\geq (A_M - \tfrac{A_M - A_m}{4})e^{-B(\tau-t')} + m_{\mathcal{N}}(t_0) - A_m e^{-B(\tau-t')} \\ &\geq m_{\mathcal{N}}(t_0) + \tfrac{3}{4}(A_M - A_m)e^{-B\Delta} \\ &\geq m_{\mathcal{N}}(t_0) + \eta \end{aligned}$$

[4]The solutions of the normal nodes' trajectories are understood in the sense of Carathéodory. Hence, it is possible that the derivative of the solution does not exist on a set of points in time of Lebesgue measure zero.

where we have used the fact that $\Delta < \ln(3)/B$ in the last line. Similarly, using (10), it follows that for $\tau \in [t, t']$

$$\begin{aligned} x_i(\tau) &> (M_{\mathcal{N}}(t_0) - \eta)e^{B(t'-\tau)} + M_{\mathcal{N}}(\tau)(1 - e^{B(t'-\tau)}) \\ &\geq M_{\mathcal{N}}(\tau) - \tfrac{A_M - A_m}{4} e^{B\Delta} \\ &> A_M - \tfrac{3}{4}(A_M - A_m) \\ &\geq A_m + \tfrac{1}{4}(A_M - A_m) \\ &\geq m_{\mathcal{N}}(t_0) + \eta. \end{aligned}$$

Therefore, $i \notin \mathcal{X}_m(t, t_0, \Delta, \eta)$. Conversely, suppose $i \in \mathcal{N} \cap \mathcal{X}_m(t, t_0, \Delta, \eta)$. Then, $\exists t' \in [t, t + \Delta]$ such that $x_i(t') < m_{\mathcal{N}}(t_0) + \eta$. It follows from (9) that for $\tau \in [t', t + \Delta]$

$$\begin{aligned} x_i(\tau) &< (m_{\mathcal{N}}(t_0) + \eta)e^{-B(\tau - t')} + M_{\mathcal{N}}(t_0)(1 - e^{-B(\tau - t')}) \\ &\leq M_{\mathcal{N}}(t_0) - (M_{\mathcal{N}}(t_0) - m_{\mathcal{N}}(t_0))e^{-B\Delta} + \eta e^{-B\Delta} \\ &\leq M_{\mathcal{N}}(t_0) - \tfrac{3}{4}(A_M - A_m)e^{-B\Delta} \\ &< M_{\mathcal{N}}(t_0) - \eta. \end{aligned}$$

Finally, using (12), it follows that for $\tau \in [t, t']$

$$\begin{aligned} x_i(\tau) &< (m_{\mathcal{N}}(t_0) + \eta)e^{B(t'-\tau)} + m_{\mathcal{N}}(\tau)(1 - e^{B(t'-\tau)}) \\ &\leq m_{\mathcal{N}}(\tau) + \tfrac{A_M - A_m}{4} e^{B\Delta} \\ &< A_m + \tfrac{3}{4}(A_M - A_m) \\ &\leq A_M - \tfrac{A_M - A_m}{4} \\ &\leq M_{\mathcal{N}}(t_0) - \eta. \end{aligned}$$

Thus, $i \notin \mathcal{X}_M(t, t_0, \Delta, \eta)$. ■

C. Proof of Theorem 1

Proof: [Sufficiency]. If $M_{\mathcal{N}}(t') = m_{\mathcal{N}}(t')$, then the normal agents remain in agreement since the right side of (2) is zero for all $t \geq t'$. Thus, suppose $A_M - A_m > 0$. Note that $\Psi(t) = M_{\mathcal{N}}(t) - m_{\mathcal{N}}(t) \geq A_M - A_m \forall t$. The goal is to contradict this inequality using an induction argument applied sufficiently close to convergence of $M_{\mathcal{N}}(t)$ and $m_{\mathcal{N}}(t)$, which will show that $\Psi(t)$ shrinks smaller than $A_M - A_m$. For each $\epsilon > 0$, there exists $t_\epsilon > 0$ such that $M_{\mathcal{N}}(t) < A_M + \epsilon$ and $m_{\mathcal{N}}(t) > A_m - \epsilon \ \forall t \geq t_\epsilon$. Let $\epsilon_0 = (A_M - A_m)/4$, $\nu < (A_M - A_m)/2$, and $\Delta < \min\{\delta(\nu), \ln(3)/B\}$. Recall that $N = |\mathcal{N}|$, $B = \beta(n - F - 1)$, and $0 < \alpha \leq w_{(j,i)}(t) \leq \beta$ for all weights. Fix ϵ such that

$$0 < \epsilon < \frac{1}{2}\left[\frac{\alpha}{B}(1 - e^{-B\Delta})e^{-B\Delta}\right]^{2N} \epsilon_0. \tag{13}$$

Define $\epsilon_l = [\frac{\alpha}{B}(1 - e^{-B\Delta})e^{-B\Delta}]^{2l}\epsilon_0$ for $l \in \mathbb{Z}_{\geq 0}$, which results in $\epsilon_{l+1} = [\frac{\alpha}{B}(1 - e^{-B\Delta})e^{-B\Delta}]^2\epsilon_l$ so that $\epsilon_0 > \epsilon_1 > \ldots > \epsilon_{N-1} > 2\epsilon > 0$. For brevity, define $\mathcal{X}_M^l = \mathcal{X}_M(t_\epsilon + \Delta l, t_\epsilon, \Delta, \epsilon_l)$ and $\mathcal{X}_m^l = \mathcal{X}_m(t_\epsilon + \Delta l, t_\epsilon, \Delta, \epsilon_l)$ for $l = 0, 1, \ldots, N$. By definition, there is at least one normal node in $\mathcal{X}_M^0$ and $\mathcal{X}_m^0$, and all of the $\mathcal{X}_M^l$ and $\mathcal{X}_m^l$ are disjoint by Lemma 2. We show by induction on l that if both $\mathcal{X}_M^l \cap \mathcal{N}$ and $\mathcal{X}_m^l \cap \mathcal{N}$ are nonempty, then $|\mathcal{X}_m^{l+1} \cap \mathcal{N}| \leq |\mathcal{X}_m^l \cap \mathcal{N}|$ and $|\mathcal{X}_M^{l+1} \cap \mathcal{N}| \leq |\mathcal{X}_M^l \cap \mathcal{N}|$, and at least one of these inequalities is strict. Since $|\mathcal{X}_m^0 \cap \mathcal{N}| + |\mathcal{X}_M^0 \cap \mathcal{N}| \leq N$, there exists $T < N$ such that at least one of $\mathcal{X}_M^T \cap \mathcal{N}$ and $\mathcal{X}_m^T \cap \mathcal{N}$ is empty. If $\mathcal{X}_M^T \cap \mathcal{N} = \emptyset$, then $M_{\mathcal{N}}(t_\epsilon + T\Delta) \leq M_{\mathcal{N}}(t_\epsilon) - \epsilon_T < M_{\mathcal{N}}(t_\epsilon) - 2\epsilon$. Similarly, if $\mathcal{X}_m^T \cap \mathcal{N} = \emptyset$, then $m_{\mathcal{N}}(t_\epsilon + T\Delta) \geq m_{\mathcal{N}}(t_\epsilon) + \epsilon_T > m_{\mathcal{N}}(t_\epsilon) + 2\epsilon$. In either case, $\Psi(t_\epsilon + T\Delta) < A_M - A_m$ and we reach the desired contradiction. All that remains to show is the inductive step.

Suppose $\mathcal{X}_M^l \cap \mathcal{N} \neq \emptyset$ and $\mathcal{X}_m^l \cap \mathcal{N} \neq \emptyset$. Then, the $(F + 1, F + 1)$-robustness assumption combined with the F-total assumption imply that either $\exists i \in \mathcal{X}_M^l \cap \mathcal{N}$ or $\exists i \in \mathcal{X}_m^l \cap \mathcal{N}$ (or both) such that i has at least $F + 1$ neighbors outside of its set. Either way, there are two cases to consider: (*Case 1*) None of the $F + 1$ (or more) neighbors outside of its set are used in (2) at some time $t' \in [t_\epsilon + \Delta l, t_\epsilon + \Delta(l + 1)]$, or (*Case 2*) At least one of the $F + 1$ (or more) neighbors outside of its set are used for all $t \in [t_\epsilon + \Delta l, t_\epsilon + \Delta(l + 1)]$. In what follows we prove the inductive step whenever $\exists i \in \mathcal{X}_M^l \cap \mathcal{N}$ with at least $F + 1$ neighbors outside of its set. The argument for $i \in \mathcal{X}_m^l \cap \mathcal{N}$ follows a similar line of reasoning.

(Case 1): In this case, $x_i(t') \leq M_{\mathcal{N}}(t_\epsilon) - \epsilon_l$ (otherwise, it would use at least one of its $F + 1$ neighbors' values outside of $\mathcal{X}_M^l$). It follows from (9) that

$$x_i(t_\epsilon + \Delta(l + 1)) \leq M_{\mathcal{N}}(t_\epsilon) - \epsilon_l e^{-B\Delta}.$$

Using this with (9) to upper bound $x_i(t)$, for $t \in [t_\epsilon + \Delta(l + 1), t_\epsilon + \Delta(l + 2)]$, we see that

$$x_i(t) \leq M_{\mathcal{N}}(t_\epsilon) - \epsilon_l e^{-2B\Delta} \leq M_{\mathcal{N}}(t_\epsilon) - \epsilon_{l+1}.$$

Therefore, $i \notin \mathcal{X}_M^{l+1}$. The same reasoning shows that $j \notin \mathcal{X}_M^{l+1}$ whenever j is a normal node with $j \notin \mathcal{X}_M^l$.

(Case 2): We can bound the right-hand side of (2) by

$$\begin{aligned} \dot{x}_i(t) &\leq \alpha(M_{\mathcal{N}}(t_\epsilon) - \epsilon_l - x_i(t)) + (B - \alpha)(M_{\mathcal{N}}(t_\epsilon) - x_i(t)) \\ &\leq -Bx_i(t) + BM_{\mathcal{N}}(t_\epsilon) - \alpha\epsilon_l \end{aligned}$$

for $t \in [t_\epsilon + \Delta l, t_\epsilon + \Delta(l + 1)]$. Using this with integrating factor $e^{B(t - t_\epsilon - \Delta l)}$, and integrating over this time interval yields

$$\begin{aligned} x_i(t_\epsilon + \Delta(l+1)) &\leq x_i(t_\epsilon + \Delta l)e^{-B\Delta} + (M_{\mathcal{N}}(t_\epsilon) - \tfrac{\alpha\epsilon_l}{B})(1 - e^{-B\Delta}) \\ &\leq M_{\mathcal{N}}(t_\epsilon) - \tfrac{\alpha}{B}(1 - e^{-B\Delta})\epsilon_l. \end{aligned}$$

Using this with (9) to upper bound $x_i(t)$ for $t \in [t_\epsilon + \Delta(l + 1), t_\epsilon + \Delta(l + 2)]$, we see

$$\begin{aligned} x_i(t) &\leq M_{\mathcal{N}}(t_\epsilon) - \tfrac{\alpha}{B}(1 - e^{-B\Delta})e^{-B(t - t_\epsilon - \Delta(l+1))}\epsilon_l \\ &\leq M_{\mathcal{N}}(t_\epsilon) - \tfrac{\alpha}{B}(1 - e^{-B\Delta})e^{-B\Delta}\epsilon_l \leq M_{\mathcal{N}}(t_\epsilon) - \epsilon_{l+1}. \end{aligned}$$

Thus, $i \notin \mathcal{X}_M^{l+1}$. The final step is to show that $j \notin \mathcal{X}_m^{l+1}$ whenever j is a normal node with $j \notin \mathcal{X}_m^l$. Whenever $j \notin \mathcal{X}_m^l$, it means that $x_j(t_\epsilon + \Delta(l + 1)) \geq m_{\mathcal{N}}(t_\epsilon) + \epsilon_l$. Using this with (11) to lower bound $x_j(t)$ for $t \in [t_\epsilon + \Delta(l + 1), t_\epsilon + \Delta(l + 2)]$, we see that

$$x_j(t) \geq m_{\mathcal{N}}(t_\epsilon) + \epsilon_l e^{-B\Delta} \geq m_{\mathcal{N}}(t_\epsilon) + \epsilon_{l+1}.$$

Hence, $j \notin \mathcal{X}_m^{l+1}$, as claimed. Therefore, if $i \in \mathcal{X}_M^l \cap \mathcal{N}$ has at least $F + 1$ neighbors outside of its set, we are guaranteed that $|\mathcal{X}_M^{l+1} \cap \mathcal{N}| < |\mathcal{X}_M^l \cap \mathcal{N}|$ and $|\mathcal{X}_m^{1+1} \cap \mathcal{N}| \leq |\mathcal{X}_m^l \cap \mathcal{N}|$.

[Necessity]: If $\mathcal{D}$ is not $(F+1, F+1)$-robust, then there are nonempty, disjoint $\mathcal{S}_1, \mathcal{S}_2 \subset \mathcal{V}$ such that none of the conditions 1–3 of Definition 5 hold (with $r = F+1$ and $s = F+1$). Suppose the initial state of each node in $\mathcal{S}_1$ and $\mathcal{S}_2$ is a and b, respectively, with $a < b$. Let all other nodes have initial states taken from the interval $[a, b]$. Since $|\mathcal{X}_{\mathcal{S}_1}^{F+1}| + |\mathcal{X}_{\mathcal{S}_2}^{F+1}| \leq F$, suppose all nodes in $\mathcal{X}_{\mathcal{S}_1}^{F+1}$ and $\mathcal{X}_{\mathcal{S}_2}^{F+1}$ are adversaries that keep their states constant for $t \geq 0$. There is still at least one normal node in both $\mathcal{S}_1$ and $\mathcal{S}_2$ since $|\mathcal{X}_{\mathcal{S}_1}^{F+1}| < |\mathcal{S}_1|$ and $|\mathcal{X}_{\mathcal{S}_2}^{F+1}| < |\mathcal{S}_2|$, respectively. Therefore, each normal node in $\mathcal{S}_1$ ($\mathcal{S}_2$) removes the F or less state values greater than a (less than b) from outside $\mathcal{S}_1$ ($\mathcal{S}_2$). Hence, each normal node in $\mathcal{S}_1$ and $\mathcal{S}_2$ maintains the state of a and b, respectively. Thus, no consensus is achieved, which contradicts the assumption. ■

D. Proof of Theorem 2

Proof: Let $\Delta < \min\{\delta(\nu), \ln(3)/B, \frac{\tau}{N}\}$. Fix ϵ as in (13) and let $t'_\epsilon \geq 0$ be a point in time such that $M_{\mathcal{N}}(t) < A_M + \epsilon$ and $m_{\mathcal{N}}(t) > A_m - \epsilon$ for all $t \geq t'_\epsilon$. Define t_ϵ as the next switching time in the subsequence $\{t'_k\}$ after t'_ϵ (see case 1), or $t_\epsilon = \max\{t'_\epsilon, t'_k\}$ (see case 2). Since $\Delta < \tau/N$, the same induction argument used in the proof of Theorem 1 shows that $\Psi(t_\epsilon + T\Delta) < A_M - A_m$. ■

E. Proof of Lemma 3

Proof: Let $\bar{x}_i = Q^{-1}x_i$. Then, The closed-loop system for normal node i may be rewritten as

$$\dot{\bar{x}}_i(t) = R\bar{x}_i(t) + e^{Rt}\Phi_F\left(\{e^{-Rt}\bar{x}_j(t)\}_{j\in\mathcal{J}_i(t)}\right).$$

We assume A has $p \geq 0$ nondefect zero eigenvalues and $2q$ simple nonzero eigenvalues on the imaginary axis. If A has $p \geq 1$ (nondefect) zero eigenvalues, then each component $\bar{x}_{i,k}(t) \in \mathbb{R}$, $k = 1, \ldots, p$, evolves as an integrator using ARC-P. It follows from Theorem 2 that there exists $\bar{x}_{0,k}(0) \in [\min_{i\in\mathcal{N}}\{\bar{x}_{i,k}(0)\}, \max_{i\in\mathcal{N}}\{\bar{x}_{i,k}(0)\}]$ and $\kappa_k : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ with $\kappa_k(t) \to 0$ as $t \to \infty$, such that for all $t \geq 0$ and for all $i \in \mathcal{N}$

$$||\bar{x}_{i,k}(t) - \bar{x}_{0,k}(0)||_2 \leq \kappa_k(t)||\bar{x}_{i,k}(0) - \bar{x}_{0,k}(0)||_2.$$

Next, consider the q oscillatory modes each with states $[\bar{x}_i]_l \triangleq [\bar{x}_{i,p+2l-1}, \bar{x}_{i,p+2l}]^{\mathsf{T}} \in \mathbb{R}^2$, for $l = 1, 2, \ldots, q$ and $i \in \mathcal{V}$, and denote $R_2(\omega_l) = R_{2,l}$ for brevity. The closed-loop system for this component is given by

$$[\dot{\bar{x}}_i]_l(t) = R_{2,l}[\bar{x}_i]_l(t) + e^{R_{2,l}t}\Phi_F\left(\{e^{-R_{2,l}t}[\bar{x}_j]_l(t)\}_{j\in\mathcal{J}_i(t)}\right).$$

Consider the change of variable

$$[z_i]_l(t) = e^{-R_{2,l}t}[\bar{x}_i]_l(t), \quad i \in \mathcal{V}.$$

Then, for all $i \in \mathcal{N}$

$$[\dot{z}_i]_l(t) = \Phi_F\left(\{[z_j]_l(t)\}_{j\in\mathcal{J}_i(t)}\right).$$

where we have used the fact that $R_{2,l}e^{-R_{2,l}t} = e^{-R_{2,l}t}R_{2,l}$. It follows from Theorem 2 that the $[z_i]_l$'s asymptotically converge to a common state, denoted $[\bar{x}_0]_l(0) \triangleq [\bar{x}_{0,p+l}(0), \bar{x}_{0,p+l+1}(0)]^{\mathsf{T}} \in \mathbb{R}^2$. Since $[z_i]_l(0) = [\bar{x}_i]_l(0)$ for all $i \in \mathcal{N}$, Theorem 2 implies that the common limit of the consensus process $[\bar{x}_0]_l(0)$ satisfies for each element $r \in \{0, 1\}$

$$\bar{x}_{0,p+2l-r}(0) \in \left[\min_{i\in\mathcal{N}}\{\bar{x}_{i,p+2l-r}(0)\}, \max_{i\in\mathcal{N}}\{\bar{x}_{i,p+2l-r}(0)\}\right].$$

Because the $[z_i]_l$'s asymptotically converge to $[\bar{x}_0]_l(0)$, there exists a positive-definite function $\kappa_{p+l} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ that satisfies $\kappa_{p+l}(t) \to 0$ as $t \to \infty$, such that for all $t \geq 0$ and for all $i \in \mathcal{N}$

$$||[z_i]_l(t) - [\bar{x}_0]_l(0)||_2 \leq \kappa_{p+l}(t)||[z_i]_l(0) - [\bar{x}_0]_l(0)||_2.$$

By multiplying each side of the inequality by $||e^{R_{2,l}t}||_2$ and using the submultiplicative property of matrix norms [41], it follows that $\forall i \in \mathcal{N}$

$$\begin{aligned}||[\bar{x}_i]_l(t) - e^{R_{2,l}t}[\bar{x}_0]_l(0)||_2 \\ \leq \kappa_{p+l}(t)||e^{R_{2,l}t}||_2||[\bar{x}_i]_l(0) - [\bar{x}_0]_l(0)||_2\end{aligned}$$

where we have also used the fact that $[z_i]_l(0) = [\bar{x}_i]_l(0)$. An important bound, derived by Dahlquist [42], is

$$||e^{At}||_2 \leq e^{\mu(A)t} \ \ \forall t \in \mathbb{R}_{\geq 0}$$

where $\mu(A)$ is the logarithmic norm of A. It is shown in [43] that $\mu(A) \leq 0$ whenever A is weakly stable.[5] Hence, it follows that there exists $\delta_l \geq 0$ such that $\forall i \in \mathcal{N}$

$$\begin{aligned}||[\bar{x}_i]_l(t) - e^{R_{2,l}t}[\bar{x}_0]_l(0)||_2 \\ \leq \kappa_{p+l}(t)e^{-\delta_l t}||[\bar{x}_i]_l(0) - [\bar{x}_0]_l(0)||_2\end{aligned}$$

Since $\kappa_{p+l}(t) \to 0$ as $t \to \infty$, resilient asymptotic synchronization is achieved for each weakly stable component $[\bar{x}_i]_l \in \mathbb{R}^2$ for $l = 1, 2, \ldots, q$ in the $\bar{x}_i$ coordinates.

Combining the aforementioned inequalities, it follows that there exists $\kappa : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ with $\kappa(t) \to 0$ as $t \to \infty$, such that for all $t \geq 0$

$$||\bar{x}_i(t) - e^{Rt}\bar{x}_0(0)||_2 \leq \kappa(t)||\bar{x}_i(0) - \bar{x}_0(0)||_2 \ \ \forall i \in \mathcal{N}$$

where the elements $\bar{x}_{0,k}$ for $k = 1, 2, \ldots, m$ have initial values that satisfy

$$\bar{x}_{0,k}(0) \in \left[\min_{i\in\mathcal{N}}\{\bar{x}_{i,k}(0)\}, \max_{i\in\mathcal{N}}\{\bar{x}_{i,k}(0)\}\right]$$

so that $x_{0,k}(0) \in [m_{\mathcal{N},k}(t), M_{\mathcal{N},k}(t)]$, where $x_0 = Q\bar{x}_0$. Finally, multiplying each side of the aforementioned inequality by $||Q||_2$, using again the submultiplicative property of matrix norms, and substituting $\bar{x}_0(t) = e^{Rt}\bar{x}_0(0)$, it follows that

$$||x_i(t) - e^{At}x_0(0)||_2 \leq \kappa(t)||Q||_2||Q^{-1}||_2||x_i(0) - x_0(0)||_2$$

for all $i \in \mathcal{N}$. Since $\lim_{t\to\infty}\kappa(t) = 0$, RAWSS is achieved. ■

[5]The matrix A is said to be *weakly stable* if all eigenvalues are in the left-half plane and no eigenvalue on the imaginary axis is defect [43].

F. Proof of Theorem 3

Proof: The dynamics of x_i and ξ_i for each normal agent $i \in \mathcal{N}$ may be rewritten as

$$\dot{x}_i(t) = (A + BK)x_i(t) - BK\xi_i(t) \tag{14}$$

$$\dot{\xi}_i(t) = A\xi_i(t) + Qe^{Rt}\Phi_F\left(\{e^{-Rt}Q^{-1}\xi_j(t)\}_{j\in\mathcal{J}_i(t)}\right). \tag{15}$$

Observe that (15) matches (5) in Lemma 3. Note that since $\eta_i(0) = 0$, it follows that $\xi_i(0) = x_i(0)$ for all $i \in \mathcal{N}$. Therefore, Lemma 3 implies that the solutions of (15) converge to a solution of $\dot{\xi}_0 = A\xi_0$ such that $\xi_0(0) \in \mathcal{S}_{0,\mathcal{N}}$. Because the ξ_i's synchronize, it follows that the consensus term in (6) converges to zero. Combining this with the fact that $A + BK$ is Hurwitz, implies that $\eta_i \to 0$ as $t \to \infty$. Thus, for any $\epsilon > 0$, there exists $T \in \mathbb{R}_{>0}$ such that for all $t > T$

$$||\xi_i(t) - e^{At}\xi_0(0)||_2 < \epsilon/2 \text{ and } ||\eta_i(t)||_2 < \epsilon/2 \text{ for all } i \in \mathcal{N}.$$

Therefore, for $t > T$

$$\begin{aligned} ||x_i(t) - e^{At}\xi_0(0)||_2 &= ||\xi_i(t) + \eta_i(t) - e^{At}\xi_0(0)||_2 \\ &\leq ||\xi_i(t) - e^{At}\xi_0(0)||_2 + ||\eta_i(t)||_2 \\ &< \epsilon, \ \ \forall i \in \mathcal{N} \end{aligned}$$

so that RAWSS is achieved. ■

G. Proof of Theorem 4

Proof: Define $e_i = x_i - \hat{x}_i$. Then, the dynamics of x_i, $\hat{\xi}_i$, and e_i for each normal agent $i \in \mathcal{N}$ may be rewritten as

$$\dot{x}_i(t) = (A + BK)x_i(t) - BK(e_i(t) + \hat{\xi}_i(t)) \tag{16}$$

$$\dot{\hat{\xi}}_i(t) = A\hat{\xi}_i(t) + Qe^{Rt}\Phi_F\left(\{e^{-Rt}Q^{-1}\hat{\xi}_j(t)\}_{j\in\mathcal{J}_i(t)}\right) \tag{17}$$

$$\dot{e}_i(t) = (A + HC)e_i(t). \tag{18}$$

Observe that (17) and (18) are decoupled from each other and from (16). Note that (17) matches (5) in Lemma 3. Since $\eta_i(0) = 0$, it follows that $\hat{\xi}_i(0) = \hat{x}_i(0)$ for all $i \in \mathcal{N}$. Therefore, Lemma 3 implies that the solutions of (17) converge to a solution of $\dot{\hat{\xi}}_0 = A\hat{\xi}_0$ such that $\hat{\xi}_0(0) \in \mathcal{S}_{0,\mathcal{N}}$ (since the $\hat{x}_i(0)$'s are in some orthotope within $\mathcal{S}_{0,\mathcal{N}}$). The e_i's converge to zero because $A + HC$ is Hurwitz. Therefore, the observer error term in (7) converges to zero. Because the $\hat{\xi}_i$'s synchronize, it follows also that the consensus term in (7) converges to zero. Combining these with the fact that $A + BK$ is Hurwitz, implies that $\eta_i \to 0$ as $t \to \infty$. Thus, for any $\epsilon > 0$, there exists $T \in \mathbb{R}_{>0}$ such that for all $t > T$

$$||\hat{\xi}_i(t) - e^{At}\hat{\xi}_0(0)||_2 < \tfrac{\epsilon}{3}, \ ||e_i(t)||_2 < \tfrac{\epsilon}{3}, \text{ and } ||\eta_i(t)||_2 < \tfrac{\epsilon}{3}$$

for all $i \in \mathcal{N}$. Therefore, for $t > T$

$$\begin{aligned} ||x_i(t) - e^{At}\hat{\xi}_0(0)||_2 &= ||\hat{x}_i(t) + e_i(t) - e^{At}\hat{\xi}_0(0)||_2 \\ &= ||\hat{\xi}_i(t) + \eta_i(t) + e_i(t) - e^{At}\hat{\xi}_0(0)||_2 \\ &\leq ||\hat{\xi}_i(t) - e^{At}\hat{\xi}_0(0)||_2 + ||e_i(t)||_2 + ||\eta_i(t)||_2 \\ &< \epsilon \ \ \forall i \in \mathcal{N} \end{aligned}$$

so that RAWSS is achieved. ■

REFERENCES

[1] W. Ren, "Consensus strategies for cooperative control of vehicle formations," *IET Control Theory Appl.*, vol. 1, no. 2, pp. 505–512, 2007.

[2] Z. Lin, B. Francis, and M. Maggiore, "Necessary and sufficient graphical conditions for formation control of unicycles," *IEEE Trans. Autom. Control*, vol. 50, no. 1, pp. 121–127, Jan. 2005.

[3] M. Porfiri, G. Roberson, and D. Stilwell, "Tracking and formation control of multiple autonomous agents: A two-level consensus approach," *Automatica*, vol. 43, no. 8, pp. 1318–1328, 2007.

[4] A. Nedic and A. Olshevsky, "Distributed optimization over time-varying directed graphs," *IEEE Trans. Autom. Control*, vol. 60, no. 3, pp. 601–615, Mar. 2015.

[5] L. Xiao, S. Boyd, and S. Lall, "A scheme for robust distributed sensor fusion based on average consensus," in *Proc. 4th Int. Symp. Inf. Process. Sensor Netw.*, Apr. 2005, pp. 63–70.

[6] I. D. Schizas, A. Ribeiro, and G. B. Giannakis, "Consensus in ad hoc WSNs with noisy links Part I: Distributed estimation of deterministic signals," *IEEE Trans. Signal Process.*, vol. 56, no. 1, pp. 350–364, Jan. 2008.

[7] R. Olfati-Saber, "Distributed kalman filter with embedded consensus filters," in *Proc. IEEE 44th Conf. Dec. Control*, 2005, pp. 8179–8184.

[8] C. Liao and P. Barooah, "Disync: Accurate distributed clock synchronization in mobile ad-hoc networks from noisy difference measurements," in *Proc. Amer. Control Conf.*, Washington, DC, USA, Jun. 2013, pp. 3332–3337.

[9] J. He, P. Cheng, L. Shi, and J. Chen, "SATS: Secure average-consensus-based time synchronization in wireless sensor networks," *IEEE Trans. Signal Process.*, vol. 61, no. 24, pp. 6387–6400, Dec. 2013.

[10] F. Dorfler, M. Chertkov, and F. Bullo, "Synchronization in complex oscillator networks and smart grids," *Proc. Nat. Acad. Sci.*, vol. 110, no. 6, pp. 2005–2010, 2013.

[11] J. Cortés, "Distributed algorithms for reaching consensus on general functions," *Automatica*, vol. 44, no. 3, pp. 726–737, 2008.

[12] W. Ren and R. W. Beard, "Consensus algorithms for double-integrator dynamics," in *Distributed Consensus in Multi-Vehicle Cooperative Control: Theory and Applications*. London, U.K.: Springer, 2008, pp. 77–104.

[13] A. Abdessameud and A. Tayebi, "On consensus algorithms design for double integrator dynamics," *Automatica*, vol. 49, no. 1, pp. 253–260, 2013.

[14] L. Scardovi and R. Sepulchre, "Synchronization in networks of identical linear systems," *Automatica*, vol. 45, no. 11, pp. 2557–2562, 2009.

[15] C.-Q. Ma and J.-F. Zhang, "Necessary and sufficient conditions for consensusability of linear multi-agent systems," *IEEE Trans. Autom. Control*, vol. 55, no. 5, pp. 1263–1268, May 2010.

[16] B. A. Forouzan, *Cryptography & Network Security*. New York, NY, USA: McGraw-Hill, Inc., 2007.

[17] N. A. Lynch, *Distributed Algorithms*. San Francisco, CA, USA: Morgan Kaufmann, 1997.

[18] D. Liberzon, *Switching in Systems and Control*. Boston, MA, USA: Birkhauser, 2003.

[19] H. J. LeBlanc, H. Zhang, X. D. Koutsoukos, and S. Sundaram, "Resilient asymptotic consensus in robust networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 4, pp. 766–781, Apr. 2013.

[20] H. J. LeBlanc and X. D. Koutsoukos, "Consensus in networked multi-agent systems with adversaries," in *Proc. 14th Int. Conf. Hybrid Syst., Comput. Control*, Chicago, IL, USA, 2011, pp. 281–290.

[21] H. J. LeBlanc and X. D. Koutsoukos, "Low complexity resilient consensus in networked multi-agent systems with adversaries," in *Proc. 15th Int. Conf. Hybrid Syst., Comput. Control*, Beijing, China, 2012, pp. 5–14.

[22] H. J. LeBlanc, H. Zhang, S. Sundaram, and X. Koutsoukos, "Consensus of multi-agent networks in the presence of adversaries using only local information," in *Proc. 1st Int. Conf. High Confidence Networked Syst.*, Beijing, China, 2012, pp. 1–10.

[23] H. Zhang and S. Sundaram, "Robustness of information diffusion algorithms to locally bounded adversaries," in *Proc. Amer. Control Conf.*, Montréal, QC, Canada, 2012, pp. 5855–5861.

[24] Y. Wu, X. He, and S. Liu, "Resilient consensus for multi-agent systems with quantized communication," in *Proc. Amer. Control Conf.*, 2016, pp. 5136–5140.

[25] H. J. LeBlanc, H. Zhang, S. Sundaram, and X. Koutsoukos, "Resilient continuous-time consensus in fractional robust networks," in *Proc. Amer. Control Conf.*, 2013, pp. 1237–1242.

[26] S. M. Dibaji and H. Ishii, "Consensus of second-order multi-agent systems in the presence of locally bounded faults," *Syst. Control Lett.*, vol. 79, pp. 23–29, 2015.

[27] H. J. LeBlanc and X. Koutsoukos, "Resilient synchronization in robust networked multi-agent systems," in *Proc. 16th Int. Conf. Hybrid Syst., Comput. Control*, Philadelphia, PA, USA, 2013, pp. 21–30.
[28] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 4, pp. 1396–1407, Jul. 2014.
[29] S. Sundaram and C. N. Hadjicostis, "Distributed function calculation via linear iterative strategies in the presence of malicious agents," *IEEE Trans. Autom. Control*, vol. 56, no. 7, pp. 1495–1508, Jul. 2011.
[30] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: A system theoretic approach," *IEEE Trans. Autom. Control*, vol. 57, no. 1, pp. 90–104, Jan. 2012.
[31] A. Teixeira, H. Sandberg, and K. H. Johansson, "Networked control systems under cyber attacks with applications to power networks," in *Proc. Amer. Control Conf.*, Baltimore, MD, USA, Jul. 2010, pp. 3690–3696.
[32] L. Lamport and P. M. Melliar-Smith, "Synchronizing clocks in the presence of faults," *J. ACM*, vol. 32, no. 1, pp. 52–78, Jan. 1985.
[33] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 2, pp. 382–401, 1982.
[34] J. Hromkovic, R. Klasing, A. Pelc, P. Ruzicka, and W. Unger, *Dissemination of Information in Communication Networks*. New York, NY, USA: Springer-Verlag, 2005.
[35] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Medard, "Resilient network coding in the presence of Byzantine adversaries," in *Proc. 26th IEEE Int. Conf. Comput. Commun.*, Anchorage, AK, USA, May 2007, pp. 616–624.
[36] N. Agmon and D. Peleg, "Fault-tolerant gathering algorithms for autonomous mobile robots," *SIAM J. Comput.*, vol. 36, no. 1, pp. 56–82, Jul. 2006.
[37] X. Défago, M. Gradinariu, S. Messika, and P. Raipin-Parvédy, "Fault-tolerant and self-stabilizing mobile robots gathering," in *Distributed Computing* (Lecture Notes in Computer Science), S. Dolev, Ed., Berlin, Germany: Springer, 2006, vol. 4167, pp. 46–60.
[38] Z. Bouzid, M. G. Potop-Butucaru, and S. Tixeuil, "Optimal Byzantine-resilient convergence in uni-dimensional robot networks," *Theor. Comput. Sci.*, vol. 411, no. 34-36, pp. 3154–3168, Jul. 2010.
[39] D. Dolev, N. A. Lynch, S. S. Pinter, E. W. Stark, and W. E. Weihl, "Reaching approximate agreement in the presence of faults," *J. ACM*, vol. 33, no. 3, pp. 499–516, 1986.
[40] H. Zhang, E. Fata, and S. Sundaram, "A notion of robustness in complex networks," *IEEE Trans. Control Netw. Syst.*, vol. 2, no. 3, pp. 310–320, Sep. 2015.
[41] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge, U.K.: Cambridge Univ. Press, 1990.
[42] G. Dahlquist, "Stability and error bounds in the numerical integration of ordinary differential equations," *Trans. Roy. Inst. Technol.*, vol. 130, 1959.
[43] T. Ström, "On logarithmic norms," *SIAM J. Numer. Anal.*, vol. 12, no. 5, pp. 741–753, 1975.

Heath J. LeBlanc (S'06–M'12) received the B.S. degree (Hons.) in electrical engineering from Louisiana State University, Baton Rouge, LA, USA, in 2007 and the M.S. and Ph.D. degrees in electrical engineering from Vanderbilt University, Nashville, TN, USA, in 2010 and 2012, respectively.

He is an Assistant Professor with the Electrical & Computer Engineering and Computer Science Department, Ohio Northern University, Ada, OH, USA. His research interests include cooperative control of networked multiagent systems, resilient and fault-tolerant control, localization in vehicular ad hoc networks, and networked control systems.

Dr. LeBlanc received the Best Student Paper Award in the area of Intelligent Control Systems and Optimization at the 2010 International Conference on Informatics in Control, Automation and Robotics, and an Honorable Mention Paper Award at the 2012 International Conference on Hybrid Systems: Computation & Control.

Xenofon Koutsoukos (S'96–M'00–SM'07) received the Ph.D. degree in electrical engineering from the University of Notre Dame, Notre Dame, IN, USA, in 2000.

He is a Professor with the Department of Electrical Engineering and Computer Science, Vanderbilt University. Nashville, TN, USA. He is also a Senior Research Scientist with the Institute for Software Integrated Systems, Nashville, TN. Before joining Vanderbilt, he was a member of the Research Staff in the Xerox Palo Alto Research Center (2000–2002). His research work is in the area of cyber-physical systems with emphasis on formal methods, distributed algorithms, security and resilience, diagnosis and fault tolerance, and adaptive resource management. He has published numerous journal and conference papers and he is a coinventor of four U.S. patents.

Dr. Koutsoukos received the NSF Career Award in 2004, the Excellence in Teaching Award in 2009 from the Vanderbilt University School of Engineering, and the 2011 NASA Aeronautics Research Mission Directorate Associate Administrator Award in Technology and Innovation.