Resilient Synchronization in Robust Networked Multi-Agent Systems

Heath J. LeBlanc
Department of Electrical & Computer
Engineering and Computer Science
Ohio Northern University
Ada, OH, USA
h-leblanc@onu.edu

Xenofon Koutsoukos
Department of Electrical Engineering and
Computer Science
Vanderbilt University
Nashville, TN, USA
xenofon.koutsoukos@vanderbilt.edu

ABSTRACT

In this paper, we study local interaction rules that enable a network of dynamic agents to synchronize to a common zero-input state trajectory despite the malicious influence of a subset of adversary agents. The agents in the networked system influence one another by sharing state or output information according to a directed, time-varying graph. The normal agents have identical dynamics modeled by linear time-invariant (LTI) systems that are weakly stable, stabilizable, and detectable. The adversary agents are assumed to be omniscient and can take any uniformly continuous state or output trajectory. We design dynamic state and output control laws under the assumption that there is either an upper bound on the number of neighbors that may be adversaries, or an upper bound on the total number of adversary agents in the network. The control laws use only local information (i.e., information from neighbors in the network) and are resilient in the sense that they are able to mitigate the malicious influence of the adversary nodes and facilitate asymptotic synchronization of the normal agents. The conditions on the network topology required for the success of the synchronization control laws are specified in terms of network robustness. Network robustness is a novel topological property that codifies the notion of sufficient redundancy of directed edges between subsets of nodes in the network.

Categories and Subject Descriptors

C.2.4 [**Computer-Communication Networks**]: Distributed Systems; H.1.1 [**Models and Principles**]: Systems and Information Theory—*General Systems Theory*; C.4 [**Performance of Systems**]: Fault tolerance

General Terms

Algorithms, Security, Theory

Keywords

Synchronization, Networked multi-agent system, Resilience, Adversary

1. INTRODUCTION

Synchronization, like consensus, is a group objective where the agents seek to agree on their state values. Synchronization differs from consensus in the fact that the state values *dynamically change in the absence of influence from neighboring agents in the network*. Whereas consensus is an agreement process on *values*, synchronization is an agreement process on *the underlying dynamics*. Most often, synchronization phenomena arise in physical or biological systems where complex interactions in the coupled dynamics of the underlying physical processes cause the agents to synchronize. At times this behavior is undesirable and even harmful, such as the synchronization that occurs in the brain of an epileptic patient. Other times, synchronization is explicitly sought, and appropriate control laws or algorithms are designed to drive the agents to synchrony [23, 31].

A major challenge in the synchronization objective in multi-agent networks is the design of local coupling rules (controllers) that facilitate synchronization of the agents' dynamics. One aspect to this challenge 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. Of course, this is a common issue with consensus objectives. A second aspect, unique to synchronization, is the complication of nonlinear, possibly chaotic, agent dynamics [24]. Further, if the agents are not identical, then synchronization to common dynamics may not even be feasible, e.g., if the individual agents have no common equilibrium and a synchronization manifold does not exist [31]. Instead, in these cases, the error dynamics of each agent with respect to the *average dynamics* should be bounded near the origin [31].

Another major challenge is achieving synchronization resiliently in the presence of compromised nodes, or adversaries. It is not difficult to imagine the damage that could be caused by an adversary insinuated into a networked multi-agent system with synchronization algorithms that are not resilient. Instead of losing only the infected nodes, the entire networked system could be destroyed. Therefore, the formulation of resilient synchronization problems and the design of controllers that ensure resilience are of utmost importance.

In this paper, we introduce a resilient asymptotic synchronization (RAS) problem for the case when the normal agents are linear time-invariant (LTI) systems. It is assumed that each LTI system is weakly stable, stabilizable, and detectable. The goal is for each normal agent to asymptotically synchronize to a common, safe, zero-input solution of the system despite the influence of adversary agents. The adversaries studied here are omniscient, but are limited

in how they are able to influence the normal agents.[1] Specifically, the adversary agents cannot be duplicitous and the signals shared must satisfy certain continuity assumptions. Further, we assume an upper bound either on the number of neighbors that may be adversaries, or on the total number of adversary agents in the network. 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 main update rule of the Adversarial Robust Consensus Protocol (ARC-P), introduced in [13] and extended in [14, 16], is used as part of the resilient synchronization controllers in order to ensure resilience to adversaries. The main results provide sufficient conditions on the network topology under which RAS is achieved even for a class of dynamically switching network topologies. The class of network topologies are those that have sufficient robustness, which is a novel topological property that captures the notion of sufficient redundancy of directed edges between subsets of nodes [15, 16, 30].

The rest of the paper is organized as follows. Section 2 describes some related work. Section 3 defines the system model, the normal agent dynamics, the adversary model, and the RAS problem statement. Section 4 reviews several topics used in the resilient control design and analysis, including ARC-P, a modified Jordan form that is useful for the resilient control laws, and network robustness. Section 5 describes the controllers and provides the analysis showing the resilience of the control laws to the influence of the adversaries. Finally, Section 6 concludes the paper.

2. RELATED WORK

The research most closely related to this work is the synchronization results of [23] and the resilient consensus results of [13, 14, 16, 30]. In [23], synchronization of identical linear systems is studied under similar assumptions on the normal agents. However, in [23], it is assumed that all agents cooperate in the synchronization process (i.e., all agents are normal). Here we remove this assumption and allow for the possibility that a subset of the agents seek to disrupt the synchronization process. On the other hand, while the previous work on resilient consensus deals with adversaries, the dynamics of the normal agents are the special case of an LTI system with $A = 0$, $B = C = I$. Therefore, the results of this paper are a strict generalization of those of resilient consensus [13, 14, 16, 30].

The synchronization control laws proposed in this paper rely on our previous resilient consensus results (specifically [16]) and ideas from [23]. The most important idea borrowed from [23] is the reduction of synchronization to consensus by an appropriate change of variables involving the matrix exponential. The introduction of the matrix exponential in the change of variables is not an issue in [23] because the control law is linear and does not involve the matrix exponential. Instead, the matrix exponential and its inverse are used only in the analysis (and in fact cancel). To adapt this idea to resilient synchronization using the piecewise linear resilient consensus filter (ARC-P) requires explicit use of the matrix exponential (and its inverse) in the control law. For numerical stability, we cannot use this technique on the stable modes of the system. For this reason, we decouple the modes of the system using a modified Jordan form of the system matrix and resiliently synchronize the weakly stable modes while allowing the stable modes to die out unforced. For the integrator modes, the resilient consensus filter may be applied directly to achieve synchronization. The undamped

modes are paired as second-order oscillators so the matrix exponential is just a time-varying rotation matrix (and therefore numerically stable and easily calculated). For these modes, the change of variables used in [23] combined with ARC-P is shown to achieve resilient synchronization.

Another similar line of research is that of resilient clock synchronization, which has been studied [10, 17, 18]. However, these techniques achieve agreement resiliently on logical clock values, instead of agreement on the oscillator dynamics. The results of these papers require the assumption that the skew is negligible, since the dynamics are not directly controlled.

Finally, the research studying detection and identification of malicious nodes [21, 26, 27] is related to this work because the same threat model is assumed. In [26], a necessary condition on the connectivity of the network is given for detecting and identifying up to F malicious agents using linear iterations in synchronous networks. This condition is shown to also be sufficient for the problem by demonstrating an algorithm that can recover the initial states of the normal nodes in at most n steps. The same condition is shown to hold for the special case of consensus in [21]. In [27], detection and identification of cyber attacks on networked control systems are studied for the case of continuous-time linear systems. Attacks on nodes and on their outgoing communication channels are both studied, and it is shown that from the perspective of other nodes, the two cases are indistinguishable. As in [21], unknown input observers are used for the FDI scheme.

3. SYSTEM MODEL AND PROBLEM

Consider a time-varying network modeled by the (finite, simple) *digraph*, $\mathcal{D}(t) = (\mathcal{V}, \mathcal{E}(t))$, where $\mathcal{V} = \{1, ..., n\}$ is the *node set* and $\mathcal{E}(t) \subset \mathcal{V} \times \mathcal{V}$ is the *directed edge set* at time t. The node set is partitioned into a set of N *normal nodes* $\mathcal{N} = \{1, 2, \ldots, N\}$ and a set of M *adversary nodes* $\mathcal{A} = \{N + 1, N + 2, \ldots, n\}$, with $M = n - N$. 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 $\mathcal{N}_i^{\text{in}}(t) = \{j \in \mathcal{V} \colon (j, i) \in \mathcal{E}(t)\}$ and $\mathcal{N}_i^{\text{out}}(t) = \{j \in \mathcal{V} \colon (i, j) \in \mathcal{E}(t)\}$, respectively. The time-varying in-degree and out-degree of node i are denoted $d_i(t) = |\mathcal{N}_i^{\text{in}}(t)|$ and $d_i^{\text{out}}(t) = |\mathcal{N}_i^{\text{out}}(t)|$, respectively. The set of all digraphs on n nodes is denoted by $\Gamma_n = \{\mathcal{D}_1, \ldots, \mathcal{D}_d\}$.

The time-varying topology of the network is governed by a piecewise constant switching signal $\sigma(\cdot)$, which is defined on $\mathbb{R}_{\geq 0}$ and takes values in $\{1, \ldots, d\}$. 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 defining $\mathcal{D}_{\sigma(t)} \equiv \mathcal{D}_s$, or by simply dropping the dependence on time t.

3.1 Normal Agent Dynamics

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 linear time-invariant (LTI) system

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

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

We assume (i) A is weakly stable, (ii) (A, B) is stabilizable, and (iii) (A, C) is detectable.

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

---

$x_{j,1}, x_{j,2}, \ldots, x_{j,m}$ and $y_{j,1}, y_{j,2}, \ldots, y_{j,s}$, respectively. We denote the vector containing the k-th component of the states of all nodes in $\mathcal{N}$, $\mathcal{A}$, and $\mathcal{V}$ by

$$x_{\mathcal{N},k}(t) = [x_{1,k}(t), \ldots, x_{N,k}(t)]^\mathsf{T} \in \mathbb{R}^N,$$

$$x_{\mathcal{A},k}(t) = [x_{N+1,k}(t), \ldots, x_{n,k}(t)]^\mathsf{T} \in \mathbb{R}^M,$$

and

$$x_{\mathcal{V},k}(t) = [x_{1,k}(t), \ldots, x_{n,k}(t)]^\mathsf{T} \in \mathbb{R}^n,$$

respectively. The overall state vector of $\mathcal{N}$, $\mathcal{A}$, and $\mathcal{V}$ is denoted

$$x_{\mathcal{N}}(t) = x_{\mathcal{N}}(t) = [x_{\mathcal{N},1}^\mathsf{T}(t), \ldots, x_{\mathcal{N},m}^\mathsf{T}(t)]^\mathsf{T} \in \mathbb{R}^{Nm},$$

$$x_{\mathcal{A}}(t) = [x_{\mathcal{A},1}^\mathsf{T}(t), \ldots, x_{\mathcal{A},m}^\mathsf{T}(t)]^\mathsf{T} \in \mathbb{R}^{Mm},$$

and

$$x_{\mathcal{V}}(t) = [x_{\mathcal{V},1}^\mathsf{T}(t), \ldots, x_{\mathcal{V},m}^\mathsf{T}(t)]^\mathsf{T} \in \mathbb{R}^{nm},$$

respectively. In a similar manner, we define the k-th component of the collective *outputs* of $\mathcal{N}$, $\mathcal{A}$, or $\mathcal{V}$, and so on.

3.2 Adversary Model

The adversary model studied in this paper has two aspects: the *threat model* and the *scope of threat model*.

3.2.1 Threat Model

The threat model defines the types of behaviors allowed by individual adversary nodes. In this paper, the adversaries are assumed to be omniscient (i.e., they know all other states and the full network topology; they are aware of the system dynamics and control laws of the normal agents; they are aware of which other agents are adversaries; and they know the plans of the other adversaries[2]). However, the behavior of the adversary agents is limited by two assumptions. First, we assume each out-neighbor of an adversary agent receives the same information from the adversary. That is, the adversary agents are incapable of duplicity. A second assumption is that the signals shared by the adversary agents must be continuous functions of time. This assumption is reasonable since the output signals shared by normal agents are continuous. Therefore, it is feasible that normal agents could use discontinuities in the output signals to detect adversaries. The threat model described by these limitations is referred to as the *malicious agent*.

DEFINITION 1 (MALICIOUS AGENT). *An agent $k \in \mathcal{A}$ is a **malicious adversary** if it is omniscient, and*

- *its state and output trajectories (x_k and y_k) are continuous functions of time on $[0, \infty)$;*

- *the information conveyed to each out-neighbor is the same; i.e., $y_k(t)$ is unambiguously defined.*

The malicious adversary has been considered for the resilient consensus problem [13, 14, 16, 30] and for identification of adversaries in linear consensus networks [21, 26, 27]. Malicious adversaries are similar to Byzantine faulty nodes, which have been studied in distributed computing [11, 19], communication networks [7, 9], and mobile robotics [1, 3, 5]. As a fault model, Byzantine nodes are allowed to behave arbitrarily within the limits set by the model of computation. Therefore, the analysis requires considering worst-case behavior. The main difference between malicious and Byzantine nodes is that Byzantine nodes are capable of duplicity, i.e., the values conveyed to their out-neighbors need not be the same.

[2]One may take the viewpoint that a centralized omniscient adversary informs and directs the behavior of the individual adversary agents.

3.2.2 Scope of Threats

The scope of threat model defines the topological assumptions placed on the adversaries. In this paper, we consider two deterministic scope of threat models. The first is the F-*total model*, which assumes an upper bound $F < n$ on the total number of adversary agents in the network. The second is the F-*local model*, which assumes an upper bound F on the number of neighbors of any normal node that may be an adversary. These scope of threat models are defined as follows.

DEFINITION 2 (F-TOTAL). *A set $\mathcal{S} \subset \mathcal{V}$ is F-**total** if and only if it contains at most F nodes in the network, i.e., $|\mathcal{S}| \leq F$, $F \in \mathbb{Z}_{\geq 0}$. The F-**total model** refers to the case when the set of adversaries is an F-total set.*

DEFINITION 3 (F-LOCAL). *A set $\mathcal{S} \subset \mathcal{V}$ is F-**local** if and only if it contains at most F nodes in the neighborhood of the other nodes for all t, i.e., $|\mathcal{N}_i^{in}(t) \bigcap \mathcal{S}| \leq F$, $\forall i \in \mathcal{V} \setminus \mathcal{S}$, $F \in \mathbb{Z}_{\geq 0}$. The F-**local model** refers to the case when the set of adversaries is an F-local set.*

It should be emphasized that in time-varying network topologies, the properties defining an F-local set must hold for all points in time.

The F-total model has been studied extensively with respect to node failures in distributed computing [11, 19, 28] and mobile robotics [1, 3, 5]. The F-local model has been studied in the context of fault-tolerant (or resilient) broadcasting [8, 22, 30] and resilient consensus [30]. While the F-total model typically requires certain bounds on the fraction of nodes that may be adversaries (e.g., $n > 3F$ for Byzantine nodes [11] and $n > 2F$ for malicious nodes [12]), the F-local model is dependent on the network topology and does not imply a bound on the fraction of adversary nodes in the network.

3.3 Resilient Asymptotic Synchronization

For Resilient Asymptotic Synchronization (RAS), we consider the intervals $\mathcal{I}_{t,k}$ defined by the k-th 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 k-th 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

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

There is no explicit restriction on the initial states of the normal nodes; i.e., it is allowed that $x_i(0) \in \mathbb{R}^m$ for all $i \in \mathcal{N}$. However, it is implicitly assumed that the normal states are *safe* in the sense that they lie in some safe set $\mathcal{S}_{0,\mathcal{N}} \subset \mathbb{R}^m$. It is further assumed that the safe set $\mathcal{S}_{0,\mathcal{N}}$ contains the orthotope defined by the initial states of the normal nodes, $\mathcal{H}_{0,\mathcal{N}}$; i.e., $\mathcal{H}_{0,\mathcal{N}} \subseteq \mathcal{S}_{0,\mathcal{N}}$. With these concepts, the RAS problem is defined as follows.

DEFINITION 4. *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 **resilient asymptotic synchronization (RAS)** in the presence of adversary agents (given a particular adversary model) if there exists a 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. That is,

$$\lim_{t \to \infty} ||x_i(t) - x_0(t)||_2 = 0, \quad \forall i \in \mathcal{N}. \qquad (2)$$

A few remarks are in order with respect to the RAS problem. First, because the normal agents converge to an unforced trajectory of the system, it is important that the system has no unstable modes. However, it is possible that the matrix A in the LTI system of (1) 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 multi-agent network.

The RAS problem is related to the resilient asymptotic consensus (RAC) problem [16]. Instead of converging to a common limit as in RAC, the states of the normal agents must converge to the zero-input trajectory $x_0(t)$. 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 an unforced trajectory with an unsafe initial value.

4. PRELIMINARIES

4.1 Background

In this section we recall pertinent definitions and terminologies from matrix theory [6] and LTI system theory [2]. We use the following notations common in numerical analysis [20, 25, 29]. The set of eigenvalues of matrix $A \in \mathbb{R}^{m \times m}$ is denoted $\lambda(A) = \{\lambda \in \mathbb{C} : \det(A - \lambda I) = 0\}$. The largest real part of any eigenvalue of A is denoted $\alpha(A) = \max\{\text{Re}(\lambda) : \lambda \in \lambda(A)\}$. The dimension of the eigenspace of A corresponding to a particular eigenvalue is referred to as the *geometric multiplicity* of the eigenvalue. The multiplicity of an eigenvalue as a root of the characteristic polynomial of A is called the *algebraic multiplicity* of the eigenvalue. If the geometric multiplicity of any eigenvalue of A is strictly less than its algebraic multiplicity, then A is said to be *defective*. Such an eigenvalue (with smaller geometric multiplicity than algebraic multiplicity) is said to be *defect* [25]. These terminologies are used to define *stable* and *weakly stable* matrices.

DEFINITION 5 ([25]). *The matrix $A \in \mathbb{R}^{m \times m}$ is a **stable matrix** if $\alpha(A) < 0$. The matrix A is said to be **weakly stable** if it is stable or if $\alpha(A) = 0$ but no eigenvalue λ with $Re(\lambda) = \alpha(A)$ is defect.*

We refer to an eigenvalue $\lambda \in \lambda(A)$ as *stable* if $\text{Re}(\lambda) < 0$, *weakly stable* if $\text{Re}(\lambda) = 0$ but λ is *non-defect*, and *unstable* otherwise.

Throughout this paper, we use the notation $||A||_2$ to denote the spectral norm of matrix A and

$$\mu(A) = \max\{\mu : \mu \in \lambda((A^{\mathsf{H}} + A)/2)\}.$$

to denote the *logarithmic norm* of A [25], where A^{H} is the *Hermitian transpose* of A. Since $(A^{\mathsf{H}} + A)/2$ is a real-symmetric matrix, it has real eigenvalues [6], and $\mu(A) \in \mathbb{R}$. The stability of the matrix A is related to its logarithmic norm as follows.

THEOREM 1 ([25]). *A matrix $A \in \mathbb{R}^{m \times m}$ is stable (weakly stable) if and only if $\mu(A) < 0$ ($\mu(A) \leq 0$).*

4.2 A Block Diagonal Matrix Form

In this section, we present a block diagonal matrix form that proves useful in the design of our resilient synchronization control law.

LEMMA 1. *For any square, real-valued, weakly stable matrix $A \in \mathbb{R}^{m \times m}$, there exists an invertible matrix $Q \in \mathbb{R}^{m \times m}$ such that*

$$R = Q^{-1}AQ,$$

where R is a block diagonal matrix given by

$$R = \begin{bmatrix} \boldsymbol{diag}(J_{m_1}(\lambda_1), \ldots, J_{m_p}(\lambda_p)) & 0 \\ 0 & \boldsymbol{diag}(R_2(\omega_1), \ldots, R_2(\omega_q)) \end{bmatrix}. \qquad (3)$$

Each $J_{m_i}(\lambda_i) \in \mathbb{R}^{m_i \times m_i}$, for $i = 1, \ldots, p$, is a Jordan block in which eigenvalue λ_i either has negative real part or $\lambda_i = 0$. If $\lambda_i = 0$, then $m_i = 1$ and $J_{m_i}(\lambda_i)$ is a 1×1 zero matrix. The first z Jordan blocks (with $0 \leq z \leq p$) account for the zero eigenvalues. The remaining $p - z$ Jordan blocks correspond to eigenvalues with negative real part. Each $R_2(\omega_j)$, for $j = 1, 2, \ldots, q$, is a 2×2 matrix of the form

$$R_2(\omega_j) \triangleq R_2(\lambda_{p+2j-1}, \lambda_{p+2j}) = \begin{bmatrix} 0 & -\omega_j \\ \omega_j & 0 \end{bmatrix}, \qquad (4)$$

where $\lambda_{p+2j-1} = -\omega_j \mathsf{i}$ and $\lambda_{p+2j} = \omega_j \mathsf{i}$, with $\omega_j \neq 0$ and $\mathsf{i} = \sqrt{-1}$.

PROOF. Since A is weakly stable, all eigenvalues have nonpositive real parts and any eigenvalues with zero real part are non-defect. This implies that any zero eigenvalue corresponds to a 1×1 Jordan block. Further, because A is real-valued, any complex eigenvalues occur in conjugate pairs, which can be paired as in (4). The remainder of the result follows from the Jordan decomposition theorem. $\square$

Using the modified Jordan form of Lemma 1, we can change the coordinate system of an LTI system with weakly stable $A \in \mathbb{R}^{m \times m}$ so that it consists of decoupled LTI subsystems.[3] To show this, suppose $R = Q^{-1}AQ$ is the modified Jordan form of A given in Lemma 1, and consider the coordinate transformation

$$x = Q\bar{x}.$$

Then, the dynamics in terms of $\bar{x}$ are

$$\dot{\bar{x}} = R\bar{x} + B'u, \qquad (5a)$$

$$y = C'\bar{x}, \qquad (5b)$$

where $B' = Q^{-1}B$ and $C' = CQ$. Let

$$\bar{x} = \begin{bmatrix} \bar{x}_{m_1} \\ \bar{x}_{m_2} \\ \vdots \\ \bar{x}_{m_p} \\ \bar{x}_{m_{p+1}} \\ \vdots \\ \bar{x}_{m_{p+q}} \end{bmatrix} \quad \text{and} \quad B' = \begin{bmatrix} B'_{m_1} \\ B'_{m_2} \\ \vdots \\ B'_{m_p} \\ B'_{m_{p+1}} \\ \vdots \\ B'_{m_{p+q}} \end{bmatrix},$$

where $\bar{x}_{m_i} \in \mathbb{R}^{m_i}$ and $B'_{m_i} \in \mathbb{R}^{m_i \times r}$ for $i = 1, 2, \ldots, p$, and $\bar{x}_{m_{p+j}} \in \mathbb{R}^2$ and $B'_{m_{p+j}} \in \mathbb{R}^{2 \times 2}$ for $j = 1, 2, \ldots, q$. Each of these components corresponds to a block in the matrix R. Using this notation, we may rewrite the state equation (5a) above as $p + q$ decoupled state equations, where

$$\dot{\bar{x}}_{m_i} = J_{m_i}(\lambda_i)\bar{x}_{m_i} + B'_{m_i}u, \quad i = 1, 2, \ldots, p, \qquad (6a)$$

$$\dot{\bar{x}}_{m_{p+j}} = R_2(\omega_j)\bar{x}_{m_{p+j}} + B'_{m_{p+j}}u, \quad j = 1, 2, \ldots, q. \qquad (6b)$$

---

[3]Of course, any LTI system may be decoupled using the Jordan form. The utility of the decomposition described here is demonstrated in subsequent sections.
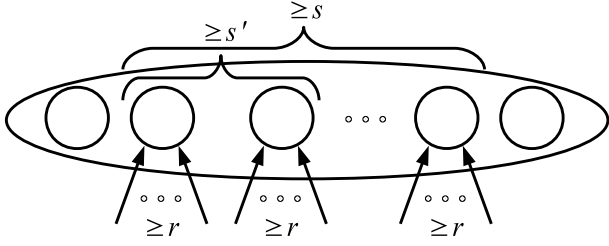
Figure 1: Illustration of an (r, s)-edge reachable set of nodes.

Note that if A has at least one zero eigenvalue (i.e., $z \geq 1$), then each $\bar{x}_{m_i} \in \mathbb{R}$ in (6a) has integrator dynamics for $i = 1, \ldots, z$. On the other hand, if A has at least one eigenvalue with negative real part, then $\bar{x}_{m_j}$ has exponentially stable dynamics for $j = z + 1, \ldots, p$.

The matrix exponential of $R_2(\omega_j)$ where $\lambda_{p+2j-1} = -\omega_j \mathrm{i}$ and $\lambda_{p+2j} = \omega_j \mathrm{i}$, with $\omega_j \neq 0$ and $\mathrm{i} = \sqrt{-1}$, is given by

$$e^{R_2(\omega_j)t} = \begin{bmatrix} \cos(\omega_j t) & -\sin(\omega_j t) \\ \sin(\omega_j t) & \cos(\omega_j t) \end{bmatrix}. \qquad (7)$$

This matrix exponential is a time-varying rotation matrix with angular frequency ω_j. The zero-input solution of the weakly stable subsystems in (6b) has the form

$$\bar{x}_{m_{p+j}}(t) = \begin{bmatrix} \cos(\omega_j t) & -\sin(\omega_j t) \\ \sin(\omega_j t) & \cos(\omega_j t) \end{bmatrix} \bar{x}_{m_{p+j}}(0), \quad j = 1, 2, \ldots, q.$$

4.3 Network Robustness

Network robustness formalizes the notion of sufficient redundancy of directed edges between subsets of nodes in the network. Therefore, this property is useful for the study of resilient distributed algorithms that use only local information. In order to define network robustness, we require the following definition [16].

DEFINITION 6 ((r, s)-EDGE REACHABLE SET). *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 $\mathcal{X}_{\mathcal{S}}^r = \{i \in \mathcal{S}: |\mathcal{N}_i^{in} \setminus \mathcal{S}| \geq r\}$, then $|\mathcal{X}_{\mathcal{S}}^r| \geq s$.*

A general illustration of an (r, s)-edge reachable set of nodes is shown in Figure 1. The parameter s in the definition of (r, s)-edge reachability quantifies a lower bound on the number of nodes in the set with at least r in-neighbors outside $\mathcal{S}$. Hence there are two forms of redundancy quantified by the definition of an (r, s)-edge reachable set (with $r, s \geq 1$). The parameter r quantifies the redundancy in the number of neighbors from outside the set, and parameter s quantifies the redundancy in the number of nodes with sufficient redundancy in the number of neighbors from outside the set. Edge reachability is used to define the global property of robustness [16], which essentially places lower bounds on the edge reachability properties of any pair of nonempty, disjoint subsets of nodes.

DEFINITION 7 ((r, s)-ROBUSTNESS). *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 $\mathcal{X}_{\mathcal{S}_k}^r = \{i \in \mathcal{S}_k: |\mathcal{N}_i^{in} \setminus \mathcal{S}_k| \geq r\}$ for $k \in \{1, 2\}$):*

(i) $|\mathcal{X}_{\mathcal{S}_1}^r| = |\mathcal{S}_1|$;

(ii) $|\mathcal{X}_{\mathcal{S}_2}^r| = |\mathcal{S}_2|$;

(iii) $|\mathcal{X}_{\mathcal{S}_1}^r| + |\mathcal{X}_{\mathcal{S}_2}^r| \geq s$.

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.

Note that an $(r, 1)$-edge reachable set is abbreviated as r-edge reachable, and an $(r, 1)$-robust digraph is abbreviated as r-robust.

4.4 Resilient Consensus Filter

In the decoupled system dynamics of (6), the subsystems corresponding to zero eigenvalues have integrator dynamics. Therefore, for these subsystems, achieving resilient synchronization is equivalent to achieving resilient consensus. This motivates the use of resilient consensus filters in the synchronization control laws. This section describes the Adversarial Robust Consensus Protocol (ARC-P) with parameter F, which has been shown to be effective in mitigating the influence of malicious adversaries under the F-total and F-local models [14, 16]. In [14, 16], ARC-P operates on scalar valued information from neighbors. In this case, ARC-P with parameter F can be described by the following operations [16].

1. At time t, each normal node i obtains the values of its in-neighbors, and forms a sorted list.

2. If there are less than F values strictly larger than its own value, $x_i(t)$, then normal node i removes all values that are strictly larger than its own. Otherwise, it removes precisely the largest F values in the sorted list. Likewise, if there are less than F values strictly smaller than its own value, then node i removes all values that are strictly smaller than its own. Otherwise, it removes precisely the smallest F values.

3. Let $\mathcal{R}_i(t)$ denote the set of nodes whose values were removed by normal node i in step 2 at time t. Each normal node i applies the update[4]

$$\dot{x}_i(t) = \sum_{j \in \mathcal{N}_i^{in}(t) \setminus \mathcal{R}_i(t)} w_{(j,i)}(t)\left(x_j(t) - x_i(t)\right), \qquad (8)$$

where the weights $w_{(j,i)}(t)$ are positive, piecewise continuous, and uniformly bounded (i.e., $0 < \epsilon \leq w_{(j,i)}(t) \leq \beta$).

To modify ARC-P with parameter F in order to handle vector valued information, simply apply the rules described above to each component of the vector. To mathematically define this behavior requires the following definitions used in the formal specification of the scalar valued version of ARC-P.

DEFINITION 8. *Let $k \in \mathbb{N}$ and $F \in \mathbb{Z}_{\geq 0}$. Denote the elements of vectors $\xi, w, z \in \mathbb{R}^k$ by ξ_l, w_l, and z_l, respectively, for $l = 1, 2, \ldots, k$. Then:*

*(i) The (ascending) **sorting function** on k elements, $\rho_k \colon \mathbb{R}^k \to \mathbb{R}^k$, is defined by $\xi = \rho_k(z)$ such that ξ is a permutation of z that satisfies*

$$\xi_1 \leq \xi_2 \leq \cdots \leq \xi_k;$$

*(ii) The **weighted zero-selective reduce function** with respect to F and k, $r_{0,F}^k \colon \mathbb{R}^k \times \mathbb{R}^k \to \mathbb{R}$, is defined by (9), where $1_{\geq 0}(\cdot)$ and $1_{\leq 0}(\cdot)$ are indicator functions, and the weights are uniformly bounded by $0 < \epsilon \leq w_l \leq \beta$, $\forall l$.*

---

[4]Note that if all neighboring values are removed, then $\dot{x}_i(t) = 0$. Furthermore, in (8) $x_j(t) \in \mathbb{R}$ for all $j \in \mathcal{V}$.

$$r_{0,F}^k(z,w) = \begin{cases} \sum_{l=1}^{F} w_l 1_{\geq 0}(z_l)z_l + \sum_{l=F+1}^{k-F} w_l z_l + \sum_{l=k-F+1}^{k} w_l 1_{\leq 0}(z_l)z_l & k > 2F; \\ \sum_{l=1}^{k-F} w_l 1_{\geq 0}(z_l)z_l + \sum_{l=F+1}^{k} w_l 1_{\leq 0}(z_l)z_l & F < k \leq 2F; \\ 0 & k \leq F; \end{cases} \tag{9}$$

(iii) The composition of the sorting and weighted zero-selective reduce functions with respect to F and k is defined by $\phi_{0,F}^k : \mathbb{R}^k \times \mathbb{R}^k \to \mathbb{R}$, which is defined for all $z \in \mathbb{R}^k$ and $w \in \mathbb{R}^k$ such that $0 < \epsilon \leq w_l \leq \beta$ by

$$\phi_{0,F}^k(z,w) = r_{0,F}^k(\rho_k(z),w).$$

Observe that whenever $k = d_i(t)$ (the in-degree of node i) and the input vector z is a vector of relative states of the form $x_j(t) - x_i(t)$, where node j is a neighbor of node i, the sorting function sorts the relative states. The zero-selective reduce function then removes up to the smallest F relative state values *only if they are negative*, or, equivalently, if the corresponding x_j is less than x_i. Likewise, it removes up to the largest F values only if they are positive (or $x_j > x_i$). The remaining values are weighted and summed. Hence, the function $\phi_{0,F}^{d_i(t)}$ performs the same operations as the right-hand side of (8) when applied to a vector containing the relative state values $x_j(t) - x_i(t)$ for $j \in \mathcal{N}_i^{\text{in}}(t)$.

To describe the vector of relative state values needed for this representation, let $1_{d_i(t)}$ denote the $d_i(t) \times 1$ vector of ones and define $N_i(t) \in \mathbb{R}^{d_i(t) \times n}$ as a sparse matrix with each row corresponding to a distinct $j \in \mathcal{N}_i^{\text{in}}(t)$ such that each row has a single 1 in the j-th column. With this notation, (8) may be rewritten as

$$\dot{x}_i(t) = \phi_{0,F}^{d_i(t)}\left(N_i(t)x_{\mathcal{V}}(t) - x_i(t)1_{d_i(t)}, w_i(t)\right),$$

where $w_i(t) \in \mathbb{R}^{d_i(t)}$ is a vector of weights of the form $w_{(j,i)}(t)$ corresponding to each $j \in \mathcal{N}_i^{\text{in}}(t)$.

We extend the definitions above to describe ARC-P with vectors $x_j(t) \in \mathbb{R}^m$ for all $j \in \mathcal{V}$ as follows. Let $z, w \in \mathbb{R}^{km}$ be composite vectors with $z = [z_1^{\mathsf{T}}, \ldots, z_m^{\mathsf{T}}]^{\mathsf{T}}$ and $w = [w_1^{\mathsf{T}}, \ldots, w_m^{\mathsf{T}}]^{\mathsf{T}}$ such that $z_i, w_i \in \mathbb{R}^k$ for $i = 1, \ldots, m$. Define $\Phi_{0,F}^{k,m} : \mathbb{R}^{km} \to \mathbb{R}^m$ such that

$$\Phi_{0,F}^{k,m}(z,w) = \begin{bmatrix} \phi_{0,F}^k(z_1, w_1) \\ \vdots \\ \phi_{0,F}^k(z_m, w_m) \end{bmatrix}. \tag{10}$$

Then, the update rule of the vector valued version of ARC-P with parameter F is given by[5]

$$\dot{x}_i = \Phi_{0,F}^{d_i(t),m}\left([I_m \otimes N_i(t)]x_{\mathcal{V}}(t) - [x_i(t) \otimes 1_{d_i(t)}], w_i(t)\right)$$

$$= \begin{bmatrix} \phi_{0,F}^{d_i(t)}\left(N_i(t)x_{\mathcal{V},1}(t) - x_{i,1}(t)1_{d_i(t)}, w_{i,1}(t)\right) \\ \vdots \\ \phi_{0,F}^{d_i(t)}\left(N_i(t)x_{\mathcal{V},m}(t) - x_{i,m}(t)1_{d_i(t)}, w_{i,m}(t)\right) \end{bmatrix}, \tag{11}$$

---

[5]Recall the definition of the Kronecker product [6]. Given $B \in \mathbb{R}^{m \times n}$ and $C \in \mathbb{R}^{p \times q}$, the *Kronecker product* $B \otimes C \in \mathbb{R}^{mp \times nq}$ is defined as

$$B \otimes C \triangleq \begin{bmatrix} b_{11}C & \ldots & b_{1n}C \\ \vdots & \ddots & \vdots \\ b_{m1}C & \ldots & b_{mn}C \end{bmatrix}.$$

for each normal node $i \in \mathcal{N}$ for $t \in \mathbb{R}_{\geq 0}$. The time-varying composite weight vector

$$w_i(t) = [w_{i,1}^{\mathsf{T}}(t), \ldots, w_{i,m}^{\mathsf{T}}(t)]^{\mathsf{T}}$$

is comprised of m vectors $w_{i,k}(t) \in \mathbb{R}^{d_i(t)}$, for $k = 1, 2, \ldots, m$, each of which contains the scalar weights corresponding to the k-th component of the relative state vectors that are kept, as determined by the sorting function. For example, if the k-th component of neighbor $j \in \mathcal{N}_i^{\text{in}}(t)$ has the second smallest value in the neighborhood of i that is kept at time t for the k-th component (as determined by the sorting function), then the second entry in the weight vector $w_{i,k}(t)$ is $w_{(j,i),k}(t)$. Note that all weights are uniformly bounded between $\alpha > 0$ and $\beta \geq \alpha$.

The main resilient consensus results from [16] that are needed for the resilient synchronization analysis are summarized by the following theorem [16].

THEOREM 2. *Consider a time-varying network modeled by a time-varying digraph $\mathcal{D}(t) = (\mathcal{V}, \mathcal{E}(t))$. In the presence of uniformly continuous malicious agents under the F-total model (or F-local model), ARC-P with parameter F achieves resilient asymptotic consensus (RAC) if there exists $t_0 \geq 0$ such that $\mathcal{D}(t)$ is $(F + 1, F + 1)$-robust (or $(2F + 1)$-robust), $\forall t \geq t_0$. In either case, $x_{i,k}(t) \in [m_{\mathcal{N},k}(0), M_{\mathcal{N},k}(0)]$ for all $k \in \{1, 2, \ldots, m\}$ and $i \in \mathcal{N}$.*

5. RAS ANALYSIS

In this section, we analyze synchronization control laws in the presence of malicious agents under the F-total and F-local models. We first introduce resilient synchronization controllers for the case of full-state feedback. Then we show how to extend the dynamic control law with output feedback.

5.1 RAS with Full State Feedback

In this section, we analyze a resilient synchronization controller for the case when A is weakly stable, the pair (A, B) is stabilizable, and full-state feedback information is available; i.e., $C = I_m$ so that $y_i = x_i$ for all $i \in \mathcal{N}$. Before analyzing the dynamic control law for the general full-state feedback case, we first consider a static controller that assumes that matrices B and C are invertible.

The resilient control laws all use the modified Jordan form of Lemma 1. For A in (1a), there exists invertible Q such that

$$R = Q^{-1}AQ$$

has the form of Lemma 1. The main idea of the resilient control law is to decouple the dynamics and allow the stable components to converge to zero unforced. The weakly stable components are the only ones that explicitly require synchronization. If $\lambda_i = 0$, for $i = 1, \ldots, z$, then these weakly stable components have integrator dynamics, and correspond to the first z blocks in R. For these components, synchronization is equivalent to consensus. The remaining weakly stable components correspond to blocks $R_2(\omega_j)$ in R, as defined in (4). For these components, we consider its matrix exponential (given in (7)), and the inverse of its matrix exponential.
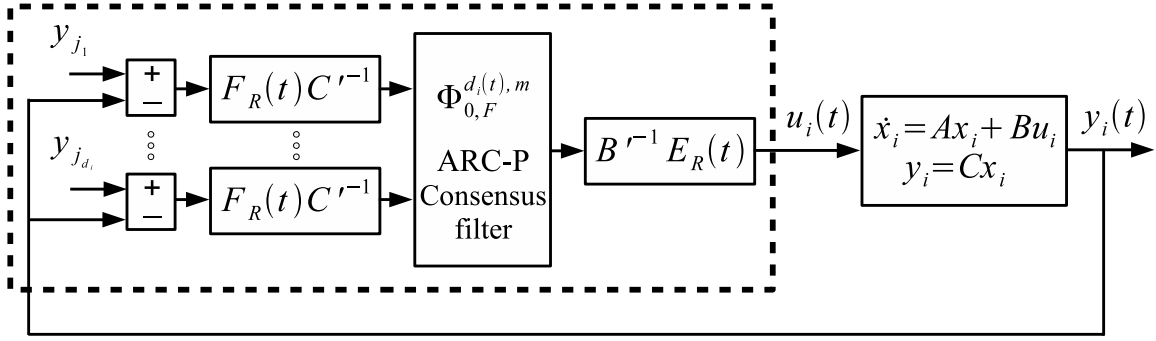
Figure 2: Resilient synchronization control law with invertible B and C for agent i.

We define the following modified exponential matrices:

$$E_R(t) = \begin{bmatrix} \mathbf{diag}(E_1, \ldots, E_p) & 0 \\ 0 & \mathbf{diag}(e^{R_2(\omega_1)t}, \ldots, e^{R_2(\omega_q)t}) \end{bmatrix} \tag{12}$$

and

$$F_R(t) = \begin{bmatrix} \mathbf{diag}(E_1, \ldots, E_p) & 0 \\ 0 & \mathbf{diag}(e^{-R_2(\omega_1)t}, \ldots, e^{-R_2(\omega_q)t}) \end{bmatrix}, \tag{13}$$

where $E_i = 1$ if $\lambda_i = 0$, and $E_i = 0$ otherwise (in the latter case, $m_i > 1$ is possible, in which case E_i is an $m_i \times m_i$ zero matrix). In either case,

$$E_R(t)F_R(t) = F_R(t)E_R(t) = \begin{bmatrix} E_1 & 0 & \ldots & 0 & 0 \\ 0 & E_2 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & E_p & 0 \\ 0 & 0 & \ldots & 0 & I_{2q} \end{bmatrix}.$$

Moreover, both $E_R(t)$ and $F_R(t)$ commute with R. That is,

$$R E_R(t) = E_R(t) R$$

and

$$R F_R(t) = F_R(t) R.$$

Now, consider the decoupled coordinates of (5) and left multiply the decoupled state vector $\bar{x}_i(t)$ by $F_R(t)$. This operation nullifies the stable components, leaves the integrator components unchanged, and transforms the components with nonzero, weakly stable eigenvalues to the corresponding component of an initial value of the unforced system $\dot{x} = Ax$. By applying the consensus filter of ARC-P to the result and then inverting the operations on the weakly stable components, we attain a control law for normal agent i of the following form:

$$u_i(t) = B'^{-1} E_R(t) \Phi_{0,F}^{d_i(t), m}(\tilde{N}_i[I_n \otimes (F_R(t)C'^{-1})]y_{\mathcal{V}}(t) \\ - [(F_R(t)C'^{-1}y_i(t)) \otimes 1_{d_i(t)}], w_i(t)), \tag{14}$$

where $\tilde{N}_i = I_m \otimes N_i$, $R = Q^{-1}AQ$ is given as in Lemma 1, $B' = Q^{-1}B$, $C' = CQ$, $E_R(t)$ is defined by (12), $F_R(t)$ is given in (13), and $\Phi_{0,F}^{d_i(t), m}(\cdot, \cdot)$ is the ARC-P function defined in (10) with $k = d_i(t)$ and parameter F. The control law of (14) is illustrated in Figure 2. Notice that matrices $E_R(t)$ and $F_R(t)$ cannot be replaced by the matrix exponential e^{Rt} and its inverse e^{-Rt}, respectively, in the case that A has stable modes. Doing so would result in numerical instability when applying the ARC-P consensus filter.

Lemma 2 given below demonstrates how the static control law of (14) is able to achieve RAS whenever the matrices B and C are invertible. The key to the success of the control law is that it reduces the resilient synchronization problem to the resilient consensus problem.

LEMMA 2. *Suppose each agent $i \in \mathcal{N}$ is an LTI system as in (1). Let $B, C \in \mathbb{R}^{m \times m}$ be nonsingular matrices and suppose that A is weakly stable. Suppose there are uniformly continuous malicious agents that satisfy either (i) the F-total, or (ii) the F-local model. Assume that the multi-agent network is time-varying and there exists $t_0 \geq 0$ such that $\mathcal{D}(t)$ is either (i) $(F+1, F+1)$-robust, or (ii) $(2F+1)$-robust, $\forall t \geq t_0$. Further, suppose each normal agent $i \in \mathcal{N}$ uses the control law of (14) for all $t \in \mathbb{R}_{\geq 0}$. Then RAS is achieved.*

PROOF. The closed-loop system for normal node i is given by

$$\dot{x}_i(t) = Ax_i(t) + QE_R(t)\Phi_{0,F}^{d_i(t), m}(\tilde{N}_i[I_n \otimes F_R(t)Q^{-1}]x_{\mathcal{V}}(t) \\ - [(F_R(t)Q^{-1}x_i(t)) \otimes 1_{d_i(t)}], w_i(t)) \tag{15}$$

Make the change in coordinates for all $i \in \mathcal{V}$

$$x_i = Q\bar{x}_i.$$

The closed-loop system may be rewritten as

$$\dot{\bar{x}}_i(t) = R\bar{x}_i(t) + E_R(t)\Phi_{0,F}^{d_i(t), m}(\tilde{N}_i[I_n \otimes F_R(t)]\bar{x}_{(\mathcal{V}, i)}(t) \\ - [(F_R(t)\bar{x}_i(t)) \otimes 1_{d_i(t)}], w_i(t)). \tag{16}$$

To facilitate analysis of the decoupled system in the $\bar{x}_i$ coordinates, let

$$\bar{x}_i = \begin{bmatrix} \bar{x}_i^{m_1} \\ \bar{x}_i^{m_2} \\ \vdots \\ \bar{x}_i^{m_p} \\ \bar{x}_i^{m_{p+1}} \\ \vdots \\ \bar{x}_i^{m_{p+q}} \end{bmatrix}, \quad i \in \mathcal{N}$$

with elements $\bar{x}_i^{m_j} = [\bar{x}_{i,1}^{m_j}, \bar{x}_{i,2}^{m_j}, \ldots, \bar{x}_{i,m_j}^{m_j}]^{\mathsf{T}} \in \mathbb{R}^{m_j}$. Notice in (16) that the stable components of $\bar{x}_i$ (i.e., $\bar{x}_i^{m_j}$ for $j = z + 1, \ldots, p$) are allowed to evolve freely, and only the weakly stable components are affected by the control law. In the following analysis, we show that each of the components $\bar{x}_i^{m_j}$ asymptotically synchronize to a corresponding component of a zero-input solution of $\dot{\bar{x}}_0 = R\bar{x}_0$ such that the initial condition of each element $\bar{x}_{0,k}$

satisfies

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

To facilitate this analysis, denote

$$\bar{x}_0 = \begin{bmatrix} \bar{x}_0^{m_1} \\ \bar{x}_0^{m_2} \\ \vdots \\ \bar{x}_0^{m_p} \\ \bar{x}_0^{m_{p+1}} \\ \vdots \\ \bar{x}_0^{m_{p+q}} \end{bmatrix}.$$

For each stable component $\bar{x}_i^{m_j} \in \mathbb{R}^{m_j}$, for $j = z+1, \ldots, p$, the Jordan block $J_{m_j}(\lambda_j)$ contains a stable eigenvalue, which implies that these components exponentially converge to zero. Thus, for *any* zero-input trajectory of

$$\dot{\bar{x}}^{m_j} = J_{m_j}(\lambda_j)\bar{x}_0^{m_j},$$

there exists $\kappa_j \colon \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ with $\kappa_j(t) \to 0$ as $t \to \infty$, such that $\forall i \in \mathcal{N}$ and for all $t \geq 0$

$$||\bar{x}_i^{m_j}(t) - e^{J_{m_j}(\lambda_j)t}\bar{x}_0^{m_j}(0)||_2 \leq \kappa_j(t)||\bar{x}_i^{m_j}(0) - \bar{x}_0^{m_j}(0)||_2.$$

In particular, there exists a zero-input solution that satisfies the above inequality with initial values $\bar{x}_{0,k}^{m_j}(0)$, for $k = 1, 2, \ldots, m_j$, such that

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

If A has $z \geq 1$ (non-defect) zero eigenvalues, then each component $\bar{x}_i^{m_k}(t) \in \mathbb{R}$, $k = 1, \ldots, z$, evolves as an integrator using ARC-P. It follows from Theorem 2 that there exists $\bar{x}_0^{m_k}(0) \in [\min_{i \in \mathcal{N}}\{\bar{x}_i^{m_k}(0)\}, \max_{i \in \mathcal{N}}\{\bar{x}_i^{m_k}(0)\}]$ and $\kappa_k \colon \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ with $\kappa_k(t) \to 0$ as $t \to \infty$, such that for all $t \geq 0$ and for all $i \in \mathcal{N}$

$$||\bar{x}_i^{m_k}(t) - \bar{x}_0^{m_k}(0)||_2 \leq \kappa_k(t)||\bar{x}_i^{m_k}(0) - \bar{x}_0^{m_k}(0)||_2.$$

Next, consider the remaining weakly stable components $\bar{x}_i^{m_{p+j}} \in \mathbb{R}^2$, for $j = 1, 2, \ldots, q$, and denote $R_2(\omega_j) = R_{2,j}$ for brevity. The closed-loop system for this component is given by

$$\dot{\bar{x}}_i^{m_{p+j}} = R_{2,j}\bar{x}_i^{m_{p+j}}$$
$$+ e^{R_{2,j}t}\Phi_{0,F}^{d_i(t),2}([I_2 \otimes N_i][I_n \otimes e^{-R_{2,j}t}]\bar{x}_{\mathcal{V}}^{m_{p+j}}(t)$$
$$- [(e^{-R_{2,j}t}\bar{x}_i^{m_{p+j}}(t)) \otimes 1_{d_i(t)}], w_i(t)).$$

Consider the change of variable

$$z_i^j(t) = e^{-R_{2,j}t}\bar{x}_i^{m_{p+j}}(t), \quad i \in \mathcal{V}.$$

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

$$\dot{z}_i^j = -R_{2,j}e^{-R_{2,j}t}\bar{x}_i^{m_{p+j}} + e^{-R_{2,j}t}R_{2,j}\bar{x}_i^{m_{p+j}}$$
$$+ \Phi_{0,F}^{d_i(t),2}\left([I_2 \otimes N_i]z_{\mathcal{V}}^j(t) - [z_i^j(t) \otimes 1_{d_i(t)}], w_i(t)\right)$$
$$= \Phi_{0,F}^{d_i(t),2}\left([I_2 \otimes N_i]z_{\mathcal{V}}^j(t) - [z_i^j(t) \otimes 1_{d_i(t)}], w_i(t)\right)$$

where we have used the fact that $R_{2,j}e^{-R_{2,j}t} = e^{-R_{2,j}t}R_{2,j}$ in going from the first to second equality. It follows from Theorem 2 that the z_i^j's asymptotically converge to a common value $\bar{x}_0^{m_{p+j}}(0) \in \mathbb{R}^2$. Since $z_i^j(0) = \bar{x}_i^{m_{p+j}}(0)$ for all $i \in \mathcal{N}$, Theorem 2 implies that the common limit of the consensus process

$\bar{x}_0^{m_{p+j}}(0)$ satisfies for each element $k \in \{1, 2\}$,

$$\bar{x}_{0,k}^{m_{p+j}}(0) \in \left[\min_{i \in \mathcal{N}}\{\bar{x}_{i,k}^{m_{p+j}}(0)\}, \max_{i \in \mathcal{N}}\{\bar{x}_{i,k}^{m_{p+j}}(0)\}\right].$$

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

$$||z_i^j(t) - \bar{x}_0^{m_{p+j}}(0)||_2 \leq \kappa_{p+j}(t)||z_i^j(0) - \bar{x}_0^{m_{p+j}}(0)||_2.$$

By multiplying each side of the inequality by $||e^{R_{2,j}t}||_2$ and using the submultiplicative property of matrix norms [6], it follows that $\forall i \in \mathcal{N}$

$$||\bar{x}_i^{m_{p+j}}(t) - e^{R_{2,j}t}\bar{x}_0^{m_{p+j}}(0)||_2$$
$$\leq \kappa_{p+j}(t)||e^{R_{2,j}t}||_2||\bar{x}_i^{m_{p+j}}(0) - \bar{x}_0^{m_{p+j}}(0)||_2,$$

where we have also used the fact that $z_i^j(0) = \bar{x}_i^{m_{p+j}}(0)$. An important bound, derived by Dahlquist [4], is

$$||e^{At}||_2 \leq e^{\mu(A)t}, \quad \forall t \in \mathbb{R}_{\geq 0}, \tag{17}$$

It follows from Theorem 1 and (17) that there exists $\delta_{p+j} \geq 0$ such that $\forall i \in \mathcal{N}$

$$||\bar{x}_i^{m_{p+j}}(t) - e^{R_{2,j}t}\bar{x}_0^{m_{p+j}}(0)||_2$$
$$\leq \kappa_{p+j}(t)e^{-\delta_{p+j}t}||\bar{x}_i^{m_{p+j}}(0) - \bar{x}_0^{m_{p+j}}(0)||_2,$$

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

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

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

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 above 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 $\kappa(t) \to 0$ as $t \to \infty$, RAS is achieved. $\square$

For the case when the input matrix B is not invertible, we require a dynamic controller that includes a stabilizing gain matrix K. The controller state η_i must be initially relaxed (i.e., $\eta_i(0) = 0$ for all $i \in \mathcal{N}$). The dynamic control law is given by

$$\dot{\eta}_i = (A + BK)\eta_i - QE_R\Phi_{0,F}^{d_i(t),m}(\tilde{N}_i[I_n \otimes F_RQ^{-1}]s_{\mathcal{V}}$$
$$- [(F_RQ^{-1}s_i) \otimes 1_{d_i(t)}], w_i) \tag{18}$$
$$u_i = K\eta_i,$$

where $\tilde{N}_i = I_m \otimes N_i$, $s_{\mathcal{V}} = [s_1^{\mathsf{T}}, s_2^{\mathsf{T}}, \ldots, s_n^{\mathsf{T}}]^{\mathsf{T}}$, $s_j = x_j - \eta_j$ for $j \in \mathcal{V}$, $E_R(t)$ is defined by (12), $F_R(t)$ is given in (13), and $\Phi_{0,F}^{d_i(t),m}(\cdot, \cdot)$ is the filter applied in ARC-P and defined in (10) with $k = d_i(t)$.

THEOREM 3. *Suppose each agent $i \in \mathcal{N}$ is an LTI system as in (1) with full-state feedback (i.e., $C = I_m$). Suppose there are malicious agents with uniformly continuous state x_k and controller state η_k for $k \in \mathcal{A}$ that satisfy either (i) the F-total, or (ii) the F-local model. Assume that A is weakly stable, the pair (A, B) is stabilizable, and let $K \in \mathbb{R}^{m \times r}$ be a stabilizing matrix such that $A + BK$ is Hurwitz. Assume that the multi-agent network is time-varying and there exists $t_0 \geq 0$ such that $\mathcal{D}(t)$ is either (i) $(F + 1, F + 1)$-robust, or (ii) $(2F + 1)$-robust, $\forall t \geq t_0$. Further, suppose each normal agent $i \in \mathcal{N}$ executes the control law of (18) with controller state η_i that is initially relaxed (i.e., $\eta_i(0) = 0$ for all $i \in \mathcal{N}$). Then RAS is achieved.*

PROOF. The dynamics of x_i and s_i for each normal agent $i \in \mathcal{N}$ may be rewritten as

$$\dot{x}_i(t) = (A + BK)x_i(t) - BK s_i(t) \tag{19}$$

$$\dot{s}_i(t) = As_i(t) + QE_R(t)\Phi_{0,F}^{d_i(t),m}(\tilde{N}_i[I_n \otimes F_R(t)Q^{-1}]s_{\mathcal{V}}(t)$$
$$- [(F_R(t)Q^{-1}s_i(t)) \otimes 1_{d_i(t)}], w_i(t)) \tag{20}$$

Observe that (20) is decoupled from (19) and matches (15) in the proof of Lemma 2. Note that since $\eta_i(0) = 0$, it follows that $s_i(0) = x_i(0)$ for all $i \in \mathcal{N}$. Therefore, Lemma 2 implies that the solutions of (20) converge to a solution of $\dot{s}_0 = As_0$ such that $s_0(0) \in \mathcal{S}_{0,\mathcal{N}}$. Because the s_i's synchronize, it follows that the consensus term in (18) 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 $t > T$,

$$||s_i(t) - e^{At}s_0(0)||_2 < \epsilon/2 \text{ and } ||\eta_i(t)|| < \epsilon/2 \text{ for all } i \in \mathcal{N}.$$

Therefore, for $t > T$

$$||x_i(t) - e^{At}s_0(0)||_2 = ||s_i(t) + \eta_i(t) - e^{At}s_0(0)||_2$$
$$\leq ||s_i(t) - e^{At}s_0(0)||_2 + ||\eta_i(t)||_2$$
$$< \epsilon \; \forall i \in \mathcal{N},$$

so that RAS is achieved. $\square$

Notice that both assumptions (i) A weakly stable and (ii) (A, B) stabilizable are needed in the proof given the dynamic control law (18). Since A is weakly stable, the dynamics of s_i in (20) reduce to the case of Lemma 2. The stabilizable pair (A, B) is used to asymptotically drive the controller state η_i to zero once the states of normal agents have synchronized.

5.2 RAS with Output Feedback

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

$$\dot{\eta}_i = (A + BK)\eta_i + H(\hat{y}_i - y_i) \tag{21}$$
$$- QE_R(t)\Phi_{0,F}^{d_i(t),m}(\tilde{N}_i[I_n \otimes F_R(t)Q^{-1}]\hat{s}_{\mathcal{V}}(t)$$
$$- [(F_R(t)Q^{-1}\hat{s}_i(t)) \otimes 1_{d_i(t)}], w_i(t))$$

$$\dot{\hat{x}}_i = A\hat{x}_i + Bu_i + H(\hat{y}_i - y_i) \tag{22a}$$
$$u_i = K\eta_i \tag{22b}$$
$$\hat{y}_i = C\hat{x}_i, \tag{22c}$$

where $\tilde{N}_i = I_m \otimes N_i$, $\hat{s}_{\mathcal{V}} = [\hat{s}_1^\mathsf{T}, \hat{s}_2^\mathsf{T}, \ldots, \hat{s}_n^\mathsf{T}]^\mathsf{T}$, $\hat{s}_j = \hat{x}_j - \eta_j$ for $j \in \mathcal{V}$, $E_R(t)$ is defined by (12), $F_R(t)$ is given in (13), and $\Phi_{0,F}^{d_i(t),m}(\cdot, \cdot)$ is the ARC-P filter defined in (10) with $k = d_i(t)$.

THEOREM 4. *Suppose each agent $i \in \mathcal{N}$ is an LTI system as in (1) with output feedback. Suppose there are malicious agents with uniformly continuous observer state $\hat{x}_k$ and controller state η_k for $k \in \mathcal{A}$ that satisfy either (i) the F-total, or (ii) the F-local model. Assume that A is weakly stable, the pair (A, B) is stabilizable, the pair (A, C) is detectable, and let $K \in \mathbb{R}^{m \times r}$ and $H \in \mathbb{R}^{m \times s}$ be a stabilizing and observer matrix, respectively, such that $A + BK$ and $A + HC$ are Hurwitz. Assume that the multi-agent network is time-varying and there exists $t_0 \geq 0$ such that $\mathcal{D}(t)$ is either (i) $(F + 1, F + 1)$-robust, or (ii) $(2F + 1)$-robust, $\forall t \geq t_0$. Further, suppose each normal agent $i \in \mathcal{N}$ executes the control law of (21) with controller state η_i that is initially relaxed (i.e., $\eta_i(0) = 0$ for all $i \in \mathcal{N}$) and Luenberger observer (22) 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 RAS is achieved.*

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

$$\dot{x}_i(t) = (A + BK)x_i(t) - BK(e_i(t) + \hat{s}_i(t)) \tag{23}$$

$$\dot{\hat{s}}_i(t) = A\hat{s}_i(t) + QE_R(t)\Phi_{0,F}^{d_i(t),m}(\tilde{N}_i[I_n \otimes F_R(t)Q^{-1}]\hat{s}_{\mathcal{V}}(t)$$
$$- [(F_R(t)Q^{-1}\hat{s}_i(t)) \otimes 1_{d_i(t)}], w_i(t)) \tag{24}$$
$$\dot{e}_i(t) = (A + HC)e_i(t) \tag{25}$$

Observe that (24) and (25) are decoupled from each other and from (23). Note that (24) matches (15) in the proof of Lemma 2. Since $\eta_i(0) = 0$, it follows that $\hat{s}_i(0) = \hat{x}_i(0)$ for all $i \in \mathcal{N}$. Therefore, Lemma 2 implies that the solutions of (20) converge to a solution of $\dot{\hat{s}}_0 = A\hat{s}_0$ such that $\hat{s}_0(0) \in \mathcal{S}_{0,\mathcal{N}}$ (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 (21) converges to zero. Because the $\hat{s}_i$'s synchronize, it follows also that the consensus term in (21) 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 $t > T$,

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

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

$$||x_i(t) - e^{At}\hat{s}_0(0)||_2 = ||\hat{x}_i(t) + e_i(t) - e^{At}\hat{s}_0(0)||_2$$
$$= ||\hat{s}_i(t) + \eta_i(t) + e_i(t) - e^{At}\hat{s}_0(0)||_2$$
$$\leq ||\hat{s}_i(t) - e^{At}\hat{s}_0(0)||_2 + ||e_i(t)||_2 + ||\eta_i(t)||_2$$
$$< \epsilon, \quad \forall i \in \mathcal{N},$$

so that RAS is achieved. $\square$

Observe that the observer error term is used in the dynamic control law of (21) to ensure the form of (24) matches (15). The assumption that (A, C) is detectable guarantees that the observer error term vanishes asymptotically.

6. CONCLUSIONS

In this paper, we introduce the resilient asymptotic synchronization (RAS) problem. We study several resilient synchronization laws under the assumption that the normal agents are identical linear time-invariant (LTI) systems that are weakly stable, stabilizable, and detectable. We demonstrate how RAS can be achieved in time-varying networks that are sufficiently robust by leveraging previous resilient consensus results. The type of adversaries considered in this paper are omniscient, and can behave arbitrarily up to certain continuity conditions. In future work, we would like to relax some of the assumptions on the normal agent dynamics and study the case of nonidentical normal agents.

7. ACKNOWLEDGMENTS

8. REFERENCES

[1] N. Agmon and D. Peleg. Fault-tolerant gathering algorithms for autonomous mobile robots. *SIAM Journal on Computing*, 36(1):56–82, July 2006.

[2] P. J. Antsaklis and A. N. Michel. *Linear systems*. McGraw-Hill,, New York, 1997.

[3] Z. Bouzid, M. G. Potop-Butucaru, and S. Tixeuil. Optimal Byzantine-resilient convergence in uni-dimensional robot networks. *Theoretical Computer Science*, 411(34-36):3154–3168, July 2010.

[4] G. Dahlquist. Stability and error bounds in the numerical integration of ordinary differential equations. In *Trans. Royal Institute of Technology*, number 130, Stockholm, Sweden, 1959.

[5] X. Défago, M. Gradinariu, S. Messika, and P. Raipin-Parvédy. Fault-tolerant and self-stabilizing mobile robots gathering. In S. Dolev, editor, *Distributed Computing*, volume 4167 of *Lecture Notes in Computer Science*, pages 46–60. Springer Berlin, Heidelberg, 2006.

[6] R. A. Horn and C. R. Johnson. *Matrix Analysis*. Cambridge University Press, 1985.

[7] J. Hromkovic, R. Klasing, A. Pelc, P. Ruzicka, and W. Unger. *Dissemination of Information in Communication Networks*. Springer-Verlag, 2005.

[8] A. Ichimura and M. Shigeno. A new parameter for a broadcast algorithm with locally bounded Byzantine faults. *Information Processing Letters*, 110:514–517, 2010.

[9] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Medard. Resilient network coding in the presence of Byzantine adversaries. In *26th IEEE International Conference on Computer Communications, INFOCOM*, pages 616–624, Anchorage, AL, May 2007.

[10] L. Lamport and P. M. Melliar-Smith. Synchronizing clocks in the presence of faults. *Journal of the ACM*, 32(1):52–78, Jan. 1985.

[11] L. Lamport, R. Shostak, and M. Pease. The Byzantine generals problem. *ACM Trans. Program. Lang. Syst.*, 4(2):382–401, 1982.

[12] H. J. LeBlanc. *Resilient Cooperative Control of Networked Multi-Agent Systems*. PhD thesis, Department of EECS, Vanderbilt University, 2012.

[13] H. J. LeBlanc and X. D. Koutsoukos. Consensus in networked multi-agent systems with adversaries. In *Proceedings of the 14th international conference on Hybrid systems: computation and control*, (HSCC '11), pages 281–290, Chicago, IL, 2011.

[14] H. J. LeBlanc and X. D. Koutsoukos. Low complexity resilient consensus in networked multi-agent systems with adversaries. In *Proceedings of the 15th international conference on Hybrid systems: computation and control*, (HSCC '12), pages 5–14, Beijing, China, 2012.

[15] H. J. LeBlanc, H. Zhang, X. D. Koutsoukos, and S. Sundaram. Resilient asymptotic consensus in robust networks. *To appear in IEEE Journal on Selected Areas in Communications, special issue on In-Network Computation: Exploring the Fundamental Limits*, 2013.

[16] 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 *Proceedings of the 1st International Conference on High Confidence Networked Systems (HiCoNS)*, pages 1–10, Beijing, China, 2012.

[17] Q. Li and D. Rus. Global clock synchronization in sensor networks. *IEEE Transactions on Computers*, 55(2):214–226, Feb. 2006.

[18] J. Lundelius and N. A. Lynch. A new fault-tolerant algorithm for clock synchronization. In *Proceedings of the 3rd ACM symposium on Principles of distributed computing*, (PODC), pages 75–88, Vancouver, British Columbia, Canada, 1984.

[19] N. A. Lynch. *Distributed Algorithms*. Morgan Kaufmann Publishers Inc., San Francisco, California, 1997.

[20] C. Moler and C. Van Loan. Nineteen dubious ways to compute the exponential of a matrix, twenty-five years later. *SIAM Review*, 45(1):3–49, 2003.

[21] F. Pasqualetti, A. Bicchi, and F. Bullo. Consensus computation in unreliable networks: A system theoretic approach. *IEEE Transactions on Automatic Control*, 57(1):90–104, Jan. 2012.

[22] A. Pelc and D. Peleg. Broadcasting with locally bounded Byzantine faults. In *Information Processing Letters*, pages 109–115, 2005.

[23] L. Scardovi and R. Sepulchre. Synchronization in networks of identical linear systems. *Automatica*, 45(11):2557–2562, 2009.

[24] S. H. Strogatz. From Kuramoto to Crawford: exploring the onset of synchronization in populations of coupled oscillators. *Physica D: Nonlinear Phenomena*, 143(1):1–20, 2000.

[25] T. Ström. On logarithmic norms. *SIAM Journal on Numerical Analysis*, 12(5):741–753, 1975.

[26] S. Sundaram and C. N. Hadjicostis. Distributed function calculation via linear iterative strategies in the presence of malicious agents. *IEEE Transactions on Automatic Control*, 56(7):1495–1508, July 2011.

[27] A. Teixeira, H. Sandberg, and K. H. Johansson. Networked control systems under cyber attacks with applications to power networks. In *Proceedings of the American Control Conference*, pages 3690–3696, Baltimore, MD, July 2010.

[28] N. H. Vaidya, L. Tseng, and G. Liang. Iterative approximate Byzantine consensus in arbitrary directed graphs. In *Proceedings of the ACM symposium on Principles of distributed computing (PODC)*, pages 365–374, Madeira, Portugal, 2012.

[29] C. Van Loan. The sensitivity of the matrix exponential. *SIAM Journal on Numerical Analysis*, 14(6):971–981, 1977.

[30] H. Zhang and S. Sundaram. Robustness of information diffusion algorithms to locally bounded adversaries. In *Proceedings of the American Control Conference*, pages 5855–5861, Montréal, Canada, 2012.

[31] J. Zhao, D. J. Hill, and T. Liu. Synchronization of dynamical networks with nonidentical nodes: Criteria and control. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 58(3):584–594, March 2011.