University of Groningen

Resilience against misbehaving nodes in asynchronous networks

Senejohnny, Danial M.; Sundaram, Shreyas; De Persis, Claudio; Tesi, Pietro

Published in:
Automatica

DOI:
[10.1016/j.automatica.2019.02.035](https://doi.org/10.1016/j.automatica.2019.02.035)

IMPORTANT NOTE: You are advised to consult the publisher's version (publisher's PDF) if you wish to cite from it. Please check the document version below.

Document Version
Publisher's PDF, also known as Version of record

Publication date:
2019

[Link to publication in University of Groningen/UMCG research database](#)

Citation for published version (APA):

Senejohnny, D. M., Sundaram, S., De Persis, C., & Tesi, P. (2019). Resilience against misbehaving nodes in asynchronous networks. *Automatica*, 104, 26-33. <https://doi.org/10.1016/j.automatica.2019.02.035>

Copyright

Other than for strictly personal use, it is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license (like Creative Commons).

The publication may also be distributed here under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license. More information can be found on the University of Groningen website: <https://www.rug.nl/library/open-access/self-archiving-pure/taverne-amendment>.

Take-down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from the University of Groningen/UMCG research database (Pure): <http://www.rug.nl/research/portal>. For technical reasons the number of authors shown on this cover page is limited to 10 maximum.

Brief paper

Resilience against misbehaving nodes in asynchronous networks[☆]Danial M. Senejohnny^{a,*}, Shreyas Sundaram^c, Claudio De Persis^a, Pietro Tesi^{b,a}^a ENTREG, University of Groningen, 9747 AG Groningen, The Netherlands^b DINFO, University of Florence, 50139 Florence, Italy^c School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN, USA

ARTICLE INFO

Article history:

Received 21 February 2018

Received in revised form 6 November 2018

Accepted 6 February 2019

Available online 11 March 2019

ABSTRACT

When dealing with network systems, a fundamental challenge is to ensure their functioning even when some of the network nodes do not operate as intended due to faults or attacks. The objective of this paper is to address the problem of resilient consensus in a context where the nodes have their own clocks, possibly operating in an asynchronous way, and can make updates at arbitrary time instants. The results represent a first step towards the development of resilient event-triggered and self-triggered coordination protocols.

© 2019 Elsevier Ltd. All rights reserved.

1. Introduction

Network systems are one of the most active research areas in engineering, as they feature a paradigm shift from centralized to distributed computation and control. A key challenge is to ensure their functioning even when some of the network units (nodes) do not operate as intended due to faults or attacks. The difficulty originates from the fact that normal (non-misbehaving) nodes can receive, process, and spread erroneous data coming from misbehaving nodes with the consequence that a failure in one point of the network can propagate through the whole network.

A prototypical problem to study resilience against misbehaving nodes is *consensus* (Cao, Yu, Ren, & Chen, 2013). In *resilient consensus*, some network nodes do not follow the coordination protocol, and the goal is to guarantee that normal (non-misbehaving) nodes can nevertheless reach consensus. Resilient consensus has been first studied by computer scientists (Dolev, Lynch, Pinter, Stark, & Weihl, 1986; Lynch, 1996), assuming that the communication graph is *complete*. With the widespread of network control applications, the problem has attracted renewed interest. LeBlanc, Zhang, Koutsoukos, and Sundaram (2013) consider *mean subsequence reduced* (MSR) consensus algorithms and provide graph-theoretic conditions for resilience under general misbehavior models. The results show

that, while the communication graph should possess a certain degree of redundancy, the completeness of the communication graph is not necessary. These results have been extended in many directions, which include time-varying networks (Saldaña, Prok, Sundaram, Campos, & Kumar, 2017), double-integrator systems (Dibaji & Ishii, 2015), sparse communication graphs (Abbas, Vorobeychik, & Koutsoukos, 2014), as well as methods for checking the robustness of specific networks (Usevitch & Panagou, 2017).

Most of the research works in this area assume that the network operates in perfect *synchrony*, meaning that all the normal nodes update at the same instants. Since this condition might be difficult to obtain, a parallel line of research has focused on ways to handle *asynchrony*, which renders consensus much more challenging to obtain (Dolev et al., 1986). Among many contributions, we mention (Dibaji & Ishii, 2017; Dibaji, Ishii, & Tempo, 2018; LeBlanc & Koutsoukos, 2012; Vaidya, Tseng, & Liang, 2012). In all these works, however, a form of synchrony remains present as the nodes either update in *rounds* (LeBlanc & Koutsoukos, 2012; Vaidya et al., 2012) or have a common sampling time (Dibaji & Ishii, 2017; Dibaji et al., 2018).

In this paper, we consider resilient consensus in a context where the nodes have independent clocks and can update at arbitrary instants. Besides the difficulties to achieve clock synchronization, one main reason for considering independent clocks is related to developments in the area of networked control where it is more and more required to adopt fully autonomous devices, which is the paradigm of *event-triggered* and *self-triggered* control (Heemels, Johansson, & Tabuada, 2012). In fact, our approach utilizes a self-triggered control scheme (De Persis & Frasca, 2013). Each node is equipped with a clock that determines when the next update is scheduled. At each update, the node collects data

[☆] The material in this paper was partially presented at the 57th IEEE Conference on Decision and Control, December 17–19, 2018, Miami Beach, Florida, USA. This paper was recommended for publication in revised form by Associate Editor Vijay Gupta under the direction of Editor Christos G. Cassandras.

* Corresponding author.

E-mail addresses: d.senejohnny@gmail.com (D.M. Senejohnny), sundara2@purdue.edu (S. Sundaram), c.de.persis@rug.nl (C. De Persis), pietro.tesi@unifi.it (P. Tesi).

from its neighbors, and determines whether it is necessary to modify its controls along with a bound on the next update instant. The main result of this paper (Theorem 1) establishes *approximate* consensus for the *F-local malicious model* (LeBlanc et al., 2013) provided that certain conditions on the network connectivity hold. These conditions can also be relaxed if misbehavior only occurs in data acquisition or timing (Theorem 2).

From a technical viewpoint, we adopt a control logic which removes “extreme” values (as in classic MSR-type algorithms) and then forms an average from a subset of the remaining values through a *quantized sign* function, which saturates the control applied at the node. This is as an approximation of the pure (non-quantized) control law of Cortés (2006) which, in the absence of misbehaving nodes, guarantees *max–min* consensus. The use of sign functions has been considered also to achieve robustness against outliers (Franceschelli, Giua, & Pisano, 2017). Although our work substantially differs from Franceschelli et al. (2017) as we do not consider a continuous data flow, both the approaches suggest that saturating the controls can be beneficial for resilience since this limits the effect of an incorrect update choice resulting from erroneous data.

2. System definition and main results

Consider a network of $n \in \mathbb{N}$ nodes interconnected in accordance with a time-invariant undirected connected graph $\mathcal{G} := (\mathcal{I}, \mathcal{E})$, where $\mathcal{I}$ is the set of nodes while $\mathcal{E} \subseteq \mathcal{I} \times \mathcal{I}$ is the set of edges. We denote the set of neighbors of $i \in \mathcal{I}$ by $\mathcal{Q}_i$, and let $d_i := |\mathcal{Q}_i|$. The set $\mathcal{Q}_i$ represents the set of nodes with which node i exchanges data. For every $i \in \mathcal{I}$, the dynamics are given by

$$\begin{cases} \dot{x}_i(t) = u_i(t) \\ z_i(t) = f_i(x_i(t)) \end{cases} \quad t \in \mathbb{R}_{\geq 0} \quad (1)$$

where $x_i \in \mathbb{R}$ is the state with $x_i(0)$ arbitrary; $u_i \in \mathbb{R}$ is the control action applied by node i ; $z_i \in \mathbb{R}$ is the output, where $f_i : \mathbb{R} \rightarrow \mathbb{R}$ is a function to be specified, and represents the value that node i makes available to its neighbors. The variable $t \in \mathbb{R}_{\geq 0}$ is understood as the *absolute* time frame within which all the nodes carry out their operations in an asynchronous way.

The objective is to design a coordination protocol in such a way that normal (non-misbehaving) nodes eventually reach *approximate* consensus despite the presence of misbehaving nodes. We will later specify the class of misbehaviors considered in this paper. According to the usual notion of consensus (Cao et al., 2013), the network nodes should converge to an equilibrium point where all the nodes have the same value lying somewhere between the minimum and maximum of their initial values. The following definition formalizes the notion of *approximate* consensus considered in this paper.

Definition 1. The network is said to reach approximate consensus if, for every initial value of the nodes, normal nodes remain between the minimum and maximum of their initial values, and there exists a constant $c \in \mathbb{R}_{>0}$ such that $\limsup_{t \rightarrow \infty} |x_i(t) - x_j(t)| < c$ for every pair (i, j) of normal nodes. ■

Network nodes carry out their operations by means of three main quantities:

- A parameter $\varepsilon \in \mathbb{R}_{>0}$, which determines the desired level of accuracy for consensus.
- A parameter $F \in \mathbb{N}$, which determines the maximum number of misbehaving neighbors that each network node is expected to encounter.

- A sequence $\{t_k^i\}_{k \in \mathbb{N}}$ of time instants at which node $i \in \mathcal{I}$ requests data from its neighbors, where $t_0^i \in [0, t_{\text{init}}]$ defines the first time instant at which node i becomes active and $t_{\text{init}} \in \mathbb{R}_{\geq 0}$ denotes the first time instant at which all the nodes are active in the network. By convention, $0 = t_0^r$ where r is the first network node to become active and $x_i(t) = x_i(t_0^i)$ for every $i \in \mathcal{I}$ and for all $t \in [0, t_0^i]$.

It is implicit in the above definition of t_{init} that *all* the nodes become active in a finite time. We will also assume that all nodes remain active for the entire runtime. The analysis can be easily generalized to the case where some of the nodes never “wake up” or “die” during the network runtime.

2.1. Coordination protocol

Let $\mathcal{N}$ and $\mathcal{M}$ represent the sets of normal nodes and misbehaving nodes, respectively, which are assumed to be time-invariant (Assumption 1 stated later). We now describe the set of operations carried out by node $i \in \mathcal{N}$. This set consists of four main operations: (i) *data acquisition*; (ii) *data transmission*; (iii) *control logic*; (iv) *timing*. These operations will also define the considered notion of misbehaviors.

(i) *Data acquisition.* At time t_k^i , node $i \in \mathcal{I}$ collects data from its neighbors. Denote by $h_i : \mathbb{R} \rightarrow \mathbb{R}$, $i \in \mathcal{I}$, the function processing the incoming data, which means that given $z_j(t)$ with $j \in \mathcal{Q}_i$, $h_i(z_j(t))$ defines the information on j available to node i at time t . For $i \in \mathcal{N}$,

$$h_i(\chi) = \chi \quad \forall \chi \in \mathbb{R}. \quad (2)$$

A data acquisition error means that (2) is not satisfied for some $\chi \in \mathbb{R}$, which represents for example a fault at the receiver.

(ii) *Data transmission.* For $i \in \mathcal{N}$, f_i in (1) satisfies

$$f_i(\chi) = \chi \quad \forall \chi \in \mathbb{R} \quad (3)$$

which means that a normal node makes available to the other nodes its true state value. A transmission error means that (3) is not satisfied for some $\chi \in \mathbb{R}$, which can represent a fault at the transmitter as well as an intentional misbehavior. By convention, node i transmits data starting at time t_0^i .

(iii) *Control logic.* The scheme is based on the idea of discarding “extreme” values (Dolev et al., 1986), which prevents normal nodes from processing potentially harmful information. For every $i \in \mathcal{I}$, let $\mathcal{D}_i(t) \subseteq \mathcal{Q}_i$ be the set of neighbors that are not discarded by i at $t \in \mathbb{R}_{\geq 0}$. For $i \in \mathcal{N}$ this set is determined as follows. Let $\mathcal{V}_i(t)$ be the ordered set formed by sorting the elements of $\mathcal{Q}_i$ in a non-decreasing order of value $h_i(z_j(t)) = z_j(t)$. An arbitrary ordering is pre-specified to classify elements with the same value. Consider the set $\mathcal{F}_i(t)$ formed by the first F elements of $\mathcal{V}_i(t)$, and let $\mathcal{E}_i(t)$ be the subset of $\mathcal{F}_i(t)$ consisting of all the elements of $\mathcal{F}_i(t)$ with associated value smaller than $x_i(t)$, that is $r \in \mathcal{E}_i(t)$ if and only if $r \in \mathcal{F}_i(t)$ and $z_r(t) < x_i(t)$. Similarly, let $\mathcal{L}_i(t)$ be the set formed by the last F elements of $\mathcal{V}_i(t)$, and let $\bar{\mathcal{E}}_i(t)$ be the subset of $\mathcal{L}_i(t)$ consisting of all the elements of $\mathcal{L}_i(t)$ with associated value larger than $x_i(t)$, that is $r \in \bar{\mathcal{E}}_i(t)$ if and only if $r \in \mathcal{L}_i(t)$ and $z_r(t) > x_i(t)$. By convention, $r \notin \mathcal{D}_i(t)$ if $t < t_0^r$, that is if node r is still not active at time t . For $i \in \mathcal{N}$, $\mathcal{D}_i(\cdot)$ satisfies

$$\mathcal{D}_i(t) = \mathcal{Q}_i \setminus (\mathcal{E}_i(t) \cup \bar{\mathcal{E}}_i(t)) \quad (4)$$

and the control action is given by

$$u_i(t) = \begin{cases} 0 & t \in [0, t_0^i) \\ \text{sign}_\varepsilon(\text{ave}_i(t_k^i)) & t \in [t_k^i, t_{k+1}^i) \end{cases} \quad (5)$$

where

$$\text{ave}_i(t) := \sum_{j \in \mathcal{D}_i(t)} (h_i(z_j(t)) - x_i(t)) \quad (6)$$

and where, for every $\chi \in \mathbb{R}$, $\text{sign}_\varepsilon(\chi) = \text{sign}(\chi)$ if $|\chi| \geq \varepsilon$ and $\text{sign}_\varepsilon(\chi) = 0$ if $|\chi| < \varepsilon$. By convention, $\mathcal{D}_i(t) = \emptyset$ implies $\text{ave}_i(t) = 0$. An error in the control logic means that (5) is not satisfied for some $t \in \mathbb{R}_{\geq 0}$.

(iv) *Timing*. For $i \in \mathcal{N}$, the next round of operations is scheduled at time $t_{k+1}^i = t_k^i + \Delta_k^i$, where

$$\begin{aligned} \Delta_k^i &\geq \underline{\Delta}_i \\ \Delta_k^i &\leq \frac{1}{4d_i} \max\{\varepsilon, |\text{ave}_i(t_k^i)|\} \end{aligned} \quad (7)$$

with $\underline{\Delta}_i \in \mathbb{R}_{>0}$ such that $\underline{\Delta}_i \leq \varepsilon/(4d_i)$. Operations can be then periodic as well as aperiodic. The first condition avoids arbitrarily fast sampling (Zeno behavior), while the second of condition is needed to reach approximate consensus. A timing error means that (7) is not satisfied for some $k \in \mathbb{N}$.

2.2. Assumptions and main results

Assumption 1. The set $\mathcal{M}$ of misbehaving nodes does not change over time, and every normal node has at most F misbehaving neighbors. ■

Assumption 2. For every $i \in \mathcal{M}$, $u_i(\cdot)$ is a locally integrable function, $\mathcal{D}_i(\cdot) \subseteq \mathcal{Q}_i$, $f_i(\cdot), h_i(\cdot) \in \mathbb{R}$ and $\Delta_k^i \geq \underline{\Delta}_i$ for all $k \in \mathbb{N}$ for some $\underline{\Delta}_i \in \mathbb{R}_{>0}$. ■

Given three distinct nodes i, j and k , k is referred to as a common neighbor of i and j if $(i, k) \in \mathcal{E}$ and $(j, k) \in \mathcal{E}$.

Assumption (Design) 3. Each pair (i, j) of normal nodes have at least $3F + 1$ neighbors in common if $(i, j) \notin \mathcal{E}$, and have at least $3F - 1$ neighbors in common if $(i, j) \in \mathcal{E}$. ■

Assumption (Design) 4. Each pair (i, j) of normal nodes have at least $2F + 1$ neighbors in common if $(i, j) \notin \mathcal{E}$, and have at least $2F - 1$ neighbors in common if $(i, j) \in \mathcal{E}$. ■

The second assumption ensures the existence of the solutions for all the nodes and for all time, that variables and functions are well defined. Assumption 2 entails no upper bound on Δ_k^i . This is in order to capture the event that a misbehaving node never collects data from its neighbors and applies an open-loop control.

We now state the main results of the paper, which are proven in Sections 4 and 5.

Theorem 1. Consider the network system (1)–(7), with the misbehaving nodes exhibiting an error in any of the operations (i)–(iv). If Assumptions 1, 2, and 3 hold true, then all the normal nodes $i \in \mathcal{N}$ remain inside the convex hull containing their initial values. Moreover, there exists a finite time $T \in \mathbb{R}_{\geq 0}$ such that $|x_i(t) - x_j(t)| < 3\varepsilon$ for all $t \geq T$ and $i, j \in \mathcal{N}$. ■

Theorem 2. Consider the network system (1)–(7), with the misbehaving nodes exhibiting an error in the operation (i) and/or (iv). If Assumptions 1, 2, and 4 hold true, then all the normal nodes $i \in \mathcal{N}$ remain inside the convex hull containing their initial values. Moreover, there exists a finite time $T \in \mathbb{R}_{\geq 0}$ such that $|x_i(t) - x_j(t)| < 3\varepsilon$ for all $t \geq T$ and $i, j \in \mathcal{N}$. ■

Intuitively, errors in data acquisition or timing are less critical as they do not alter control or output values. We note that in both Theorems 1 and 2 exact consensus is not achieved even when $F = 0$. The reason is related to the parameter ε , which must be chosen strictly positive in order to ensure that the inter-sampling times do not exhibit Zeno behavior (cf. (7)).

2.3. Discussion

Our framework covers the so-called *F-local malicious model* (LeBlanc et al., 2013). For this model, several results have been reported which establish sufficient conditions for (exact) consensus under fully or partially synchronous updates (Dibaji et al., 2018; LeBlanc & Koutsoukos, 2012; LeBlanc et al., 2013). These results hinge on the notion of *r-robustness* (LeBlanc et al., 2013), which quantifies the redundancy of information exchange between subsets of nodes needed to ensure consensus. In our paper, information redundancy is instead formalized via the concept of *common neighbors* (Assumptions 3 and 4). In this respect, we note that these assumptions are not more conservative than existing conditions based on *r-robustness* such as $(2F + 1)$ -robustness in Dibaji et al. (2018), LeBlanc et al. (2013) and $(3F + 1)$ -robustness in LeBlanc and Koutsoukos (2012). As an example, if one takes the complete graph with $n = 4$ and $F = 1$ then Assumptions 3 and 4 hold true although the network is not 3-robust.

Assumptions 3 and 4 become more conservative than those in Dibaji et al. (2018), LeBlanc and Koutsoukos (2012) and LeBlanc et al. (2013) for the *F-total malicious model*, which is a special case of the *F-local model* obtained by replacing Assumption 1 with the hypothesis that at most F nodes are misbehaving. For the *F-total model*, Dibaji et al. (2018), LeBlanc and Koutsoukos (2012) and LeBlanc et al. (2013) achieve necessary and sufficient conditions for consensus based on the notion of network $\hat{\mathcal{A}}(r, s)$ -robustness (LeBlanc et al., 2013). In this respect, it is not difficult to verify for example that Assumptions 3 and 4 imply $(F + 1, F + 1)$ -robustness, which is necessary and sufficient to ensure consensus for synchronous networks (LeBlanc et al., 2013).

In addition to the fact that they enable asynchronous update rules, Assumptions 3 and 4 are appealing also in view of the complexity related to checking them. In fact, checking these conditions simply requires to compute for each pair of nodes the intersection of their neighboring sets. Computing all the unique pairs of nodes (which are $n(n - 1)/2$ in total) can be solved in $O(n^2)$ time, while the second operation can be solved in $O(p + q) = O(n)$ time where p and q represent the cardinality of the neighboring sets of a pair of nodes. In contrast, it is computationally complex (specifically, coNP hard) to check the *r-robustness* of networks outside of certain specific cases (Usevitch & Panagou, 2017; Zhang, Fata, & Sundaram, 2017).

3. Monotonicity properties

The results of this section rely on Assumptions 1 and 2 only, and are thus independent of the specific type of node misbehavior. Let

$$x_m(t) := \min_{i \in \mathcal{N}} x_i(t), \quad x_M(t) := \max_{i \in \mathcal{N}} x_i(t) \quad (8)$$

where $t \in \mathbb{R}_{\geq 0}$. The first result shows that normal nodes remain in the convex hull containing their initial values.

Lemma 1. Consider the network system (1)–(7), and let Assumptions 1 and 2 hold. Then, $x_m(\cdot)$ and $x_M(\cdot)$ are monotonically non-decreasing and non-increasing, respectively.

Proof. We prove the statement only for $x_m(\cdot)$ since the proof for $x_M(\cdot)$ is analogous. Suppose that the claim is false, and let τ be the first time instant at which there exists a node $i \in \mathcal{N}$ such that

$$\begin{cases} x_i(\tau) \leq x_j(\tau) \quad \forall j \in \mathcal{N} \\ u_i(\tau) < 0 \end{cases} \quad (9)$$

Clearly, there could be multiple nodes achieving (9) at time τ . In this case, i is any such node. Notice that $\tau \geq t_0^i$ since $u_i(t) = 0$ for all $t \in [0, t_0^i]$.

Consider first the case where $\tau = t_k^i$ for some $k \in \mathbb{N}$. In order for $u_i(t_k^i) < 0$ we must have $\text{ave}_i(t_k^i) \leq -\varepsilon < 0$. However, this is not possible. In fact, any normal node j satisfies $z_j(t_k^i) = x_j(t_k^i) \geq x_i(t_k^i)$ because i is the node of minimum value at $\tau = t_k^i$. Hence, $z_j(t_k^i) < x_i(t_k^i)$ only if j is misbehaving. Since i has at most F misbehaving neighbors by [Assumption 1](#), if j gives $z_j(t_k^i) < x_i(t_k^i)$ then it is discarded by the control logic.

Consider next the case where τ is not an update time for node i . Let $t_k^i < \tau$ be the last update time for node i before τ . In order to have (9), there must exist a node $s \in \mathcal{N}$ such that

$$\begin{cases} x_s(t_k^i) \leq x_j(t_k^i) & \forall j \in \mathcal{N} \\ x_s(t_k^i) < x_i(t_k^i) \\ x_i(\tau) \leq x_j(\tau) & \forall j \in \mathcal{N} \\ u_i(\tau) < 0 \end{cases} \quad (10)$$

The first two conditions imply that i is not the node which takes on the minimum value at t_k^i , value which is instead attained by node s . Condition $x_s(t_k^i) < x_i(t_k^i)$ is needed otherwise $u_i(t_k^i) \geq 0$ in accordance with the previous arguments. The last three conditions mean that i becomes the minimum at τ with $u_i(\tau) = u_i(t_k^i) < 0$. Let $\beta := x_i(t_k^i) - x_s(t_k^i)$. Recall that normal nodes take controls in $\{-1, 0, 1\}$. Hence, $x_i(\tau) \leq x_j(\tau)$ for all $j \in \mathcal{N}$ only if $\tau - t_k^i \geq \beta/2$. However,

$$\begin{aligned} \Delta_k^i &\leq \frac{1}{4d_i} \sum_{j \in \mathcal{D}_i(t_k^i)} (x_i(t_k^i) - z_j(t_k^i)) \\ &\leq \frac{1}{4d_i} \sum_{j \in \mathcal{D}_i(t_k^i)} (x_i(t_k^i) - x_s(t_k^i)) \end{aligned} \quad (11)$$

The first equality follows from the fact that $u_i(t_k^i) < 0$ requires $\text{ave}_i(t_k^i) \leq -\varepsilon$ so that $\Delta_k^i \leq |\text{ave}_i(t_k^i)|/(4d_i)$. On the other hand, the second inequality follows since $z_j(t_k^i) < x_s(t_k^i)$ only if j is misbehaving, in which case it is discarded by node i in view of [Assumption 1](#) and by the control logic. Since $|\mathcal{D}_i(t)| \leq d_i$ for all $t \in \mathbb{R}_{\geq 0}$ then $\Delta_k^i \leq \beta/4$. This leads to a contradiction since it implies $\beta/2 \leq \tau - t_k^i < \Delta_k^i \leq \beta/4$ with $\beta > 0$. ■

By [Lemma 1](#), normal nodes remain in the convex hull containing their initial values. This lemma also implies that $x_m(\cdot)$ and $x_M(\cdot)$ admit a finite limit,

$$\underline{x} := \lim_{t \rightarrow \infty} x_m(t), \quad \bar{x} := \lim_{t \rightarrow \infty} x_M(t). \quad (12)$$

For the next developments, we strengthen [Lemma 1](#) by showing that there exist normal nodes that settle on the minimum and maximum values in a finite time.

Lemma 2. Consider the network system (1)–(7), and let [Assumptions 1](#) and [2](#) hold. Then, there exist at least two nodes $r, s \in \mathcal{N}$ and a finite time $T' \in \mathbb{R}_{\geq 0}$ such that $x_r(t) = \underline{x}$ and $x_s(t) = \bar{x}$ for all $t \geq T'$. In addition, $\min_{i \in \mathcal{N}} x_i(t) \geq \underline{x}$ and $\max_{i \in \mathcal{N}} x_i(t) \leq \bar{x}$ for all $t \geq T'$.

Proof. We prove the statement only for $\underline{x}$ as the proof for $\bar{x}$ is analogous. Since $x_m(\cdot)$ converges to $\underline{x}$ and is continuous, for any $\delta \in \mathbb{R}_{>0}$ there exists a finite time $T_\delta \in \mathbb{R}_{\geq 0}$ such that $|x_m(t) - \underline{x}| < \delta$ for all $t > T_\delta$. Let $\underline{\Delta} := \min_{i \in \mathcal{N}} \underline{\Delta}_i$ and pick $\delta = \underline{\Delta}/3$. Consider any $i \in \mathcal{N}$ and any update time t_k^i for node i such that $t_k^i \geq T_\delta$. Condition $t_k^i \geq T_\delta$ is well defined for any T_δ since by [Lemma 1](#) normal nodes remain in the convex hull containing their initial values so that Δ_k^i is bounded from above. We claim that, for any $i \in \mathcal{N}$ and any $t_k^i \geq T_\delta$,

$$|x_i(t_k^i) - \underline{x}| \geq \delta \Rightarrow |x_i(t) - \underline{x}| \geq \delta \quad \forall t \geq t_k^i. \quad (13)$$

In simple terms, this means that if $x_i(t_k^i)$ does not belong to $W := (\underline{x} - \delta, \underline{x} + \delta)$ then $x_i(\cdot)$ can never enter W afterwards. The implication (13) is shown as follows. Since $|x_m(t) - \underline{x}| < \delta$ for all $t > T_\delta$ then we must also have $x_j(t) > \underline{x} - \delta$ for all $t > T_\delta$ and $j \in \mathcal{N}$. This means that condition $|x_i(t_k^i) - \underline{x}| \geq \delta$ implies $x_i(t_k^i) \geq \underline{x} + \delta$. The analysis is divided into two subcases.

Case 1. Assume $x_i(t_k^i) \in [\underline{x} + \delta, \underline{x} + 2\delta]$. In this case,

$$\begin{aligned} \text{ave}_i(t_k^i) &> \sum_{j \in \mathcal{D}_i(t_k^i)} (\underline{x} - \delta - x_i(t_k^i)) > -3\delta |\mathcal{D}_i(t_k^i)| \\ &> -\varepsilon. \end{aligned} \quad (14)$$

The first inequality follows from the fact that $j \in \mathcal{D}_i(t_k^i)$ only if $z_j(t_k^i) > \underline{x} - \delta$. In fact, $z_j(t) = x_j(t) > \underline{x} - \delta$ for all $t > T_\delta$ and $j \in \mathcal{N}$. Thus, nodes with an output value less than or equal to $\underline{x} - \delta$ are misbehaving, and they are discarded in view of [Assumption 1](#) and by construction of the control logic. The second inequality follows because $x_i(t_k^i) < \underline{x} + 2\delta$ by hypothesis. The last inequality follows since $3\delta \leq \varepsilon/(4d_i)$ and $|\mathcal{D}_i(t)| \leq d_i$ for all $t \in \mathbb{R}_{\geq 0}$. Since $\text{ave}_i(t_k^i) > -\varepsilon$ implies $u_i(t) \in \{0, 1\}$ for all $t \in T_k^i$ then $x_i(t) \notin W$ for all $t \in T_k^i$, and $x_i(t_{k+1}^i) \notin W$ by continuity of $x_i(\cdot)$.

Case 2. Assume $x_i(t_k^i) \geq \underline{x} + 2\delta$. In order for node i to decrease we must have $\text{ave}_i(t_k^i) \leq -\varepsilon$. Hence,

$$\begin{aligned} \Delta_k^i &\leq \frac{1}{4d_i} \sum_{j \in \mathcal{D}_i(t_k^i)} (x_i(t_k^i) - z_j(t_k^i)) \\ &< \frac{1}{4d_i} \sum_{j \in \mathcal{D}_i(t_k^i)} (x_i(t_k^i) - \underline{x} + \delta) \leq \frac{1}{4} (x_i(t_k^i) - \underline{x} + \delta) \end{aligned} \quad (15)$$

The second inequality follows because $j \in \mathcal{D}_i(t_k^i)$ only if $z_j(t_k^i) > \underline{x} - \delta$. The third inequality follows since $|\mathcal{D}_i(t)| \leq d_i$ for all $t \in \mathbb{R}_{\geq 0}$. Since normal nodes take controls in $\{-1, 0, 1\}$, we obtain

$$x_i(t) \geq x_i(t_k^i) - \Delta_k^i \geq \underline{x} + \frac{5}{4}\delta \quad (16)$$

for all $t \in T_k^i$, where the last inequality follows from (15) and since $x_i(t_k^i) \geq \underline{x} + 2\delta$. Thus $x_i(t) \notin W$ for all $t \in T_k^i$, and $x_i(t_{k+1}^i) \notin W$ by continuity of $x_i(\cdot)$.

We conclude that if $x_i(t_k^i)$ does not belong to W for some $t_k^i \geq T_\delta$ then $x_i(\cdot)$ can never enter W afterwards. Moreover, for every $i \in \mathcal{N}$, if $x_i(t_k^i) \in W$ and $u_i(t_k^i) \neq 0$ then $x_i(t_{k+1}^i) \notin W$. In fact, in this case, node i must apply the same control input for a period not shorter than $\underline{\Delta}$. Thus, $x_i(t_{k+1}^i) \notin W$ since the control input is constant with unitary slope for at least $\underline{\Delta}$ time units and W has measure $2\delta = 2\underline{\Delta}/3$. Thus, since the number of nodes is finite, there exists a finite time $T'' \geq T_\delta$ starting from which the signal $x_i(\cdot)$, $i \in \mathcal{N}$, either persistently remains inside W or persistently remains outside W . Moreover, there exists at least one node $i \in \mathcal{N}$ for which $x_i(\cdot)$ persistently remains inside W since, by definition, $\underline{x} \in W$ is the limiting value of $x_m(\cdot)$. Consider any $x_i(\cdot)$, $i \in \mathcal{N}$, that persistently remains inside W from T'' . By the above arguments, $u_i(t_k^i) = 0$ for all $t_k^i \geq T''$. Moreover, the first sampling $t_k^i \geq T''$ must occur no later than $T' := T'' + \varepsilon/4$. In fact, either $u_i(T'') = 0$ so that $t_k^i - T'' \leq \varepsilon/(4d_i)$ by construction of the update times or $u_i(T'') \neq 0$ so that $t_k^i - T'' \leq 2\delta < \varepsilon/4$ otherwise $x_i(t_k^i) \notin W$. Hence, every $x_i(\cdot)$, $i \in \mathcal{N}$, that persistently remains inside W from T'' onwards satisfies $x_i(t) = x_i(T')$ for all $t \geq T'$. Thus $\min_{i \in \mathcal{N}} x_i(t) \geq \underline{x}$ for all $t \geq T'$ and $x_r(T') = \underline{x}$ for some $r \in \mathcal{N}$. ■

4. Generic misbehavior

By [Lemma 2](#), there exist at least two nodes $r, s \in \mathcal{N}$ and a finite time T' such that $x_r(t) = \underline{x}$ and $x_s(t) = \bar{x}$ for all $t \geq T'$. We now show that under [Assumption 3](#) $\bar{x} - \underline{x}$ is upper bounded by 3ε .

Proof of Theorem 1. The property that normal nodes always remain inside the convex hull containing their initial values has been shown in Lemma 1.

Let T' be as in Lemma 2, and denote by r and s any two nodes belonging to $\mathcal{N}$ such that $x_r(t) = \underline{x}$ and $x_s(t) = \bar{x}$ for all $t \geq T'$. Consider now any update time $t_k^r \geq T'$ for node r . Since node r does not change its value from T' onwards, we must have $\text{ave}_r(t_k^r) < \varepsilon$. This implies that $z_i(t_k^r) - x_r(t_k^r) < \varepsilon$ for all $i \in \mathcal{D}_r(t_k^r)$. In fact, in order to have $z_i(t_k^r) - x_r(t_k^r) \geq \varepsilon$ for some $i \in \mathcal{D}_r(t_k^r)$ there should exist at least one node $j \in \mathcal{D}_r(t_k^r)$ such that $z_j(t_k^r) - x_r(t_k^r) < 0$. However, this is not possible. In fact, in view of Lemma 2, $z_j(t_k^r) = x_j(t_k^r) \geq \underline{x}$ for all $j \in \mathcal{N}$ so that every node which takes on an output value smaller than $\underline{x}$ is misbehaving and it is discarded by node r in view of Assumption 1 and by construction of the control logic. Since every $i \in \mathcal{N}$ satisfies $z_i(\cdot) \equiv x_i(\cdot)$ we have $x_i(t_k^r) - \underline{x} < \varepsilon$ for all $i \in \mathcal{D}_r(t_k^r) \cap \mathcal{N}$.

Suppose first $(r, s) \notin \mathcal{E}$. Nodes r and s have at least $3F + 1$ neighbors in common by Assumption 3, so that, because of Assumption 1, they have at least $2F + 1$ neighbors in common belonging to $\mathcal{N}$. At t_k^r , node r can discard at most F normal nodes since there are no normal nodes with value smaller than $x_r(t_k^r)$. Hence, there are at least $F + 1$ normal nodes belonging to $\mathcal{D}_r(t_k^r) \cap \mathcal{Q}_s$. Starting from t_k^r , node s will sample at a time $t_k^s \leq t_k^r + \varepsilon/4$. When s will sample, it cannot discard all these $F + 1$ normal nodes by construction of the control logic and since none of these nodes can take on a value larger than $\bar{x}$ from T' onwards in view of Lemma 2. Thus at least one of these nodes, say node i , must satisfy $x_i(t_k^s) > \bar{x} - \varepsilon$ otherwise we would have $\text{ave}_s(t_k^s) \leq -\varepsilon$. Hence,

$$\begin{cases} x_i(t_k^r) < \underline{x} + \varepsilon \\ x_i(t_k^s) > \bar{x} - \varepsilon \\ x_i(t_k^s) \leq x_i(t_k^r) + \frac{\varepsilon}{4} \end{cases} \quad (17)$$

where the last inequality follows since $u_i(t) \leq 1$ for all $t \in \mathbb{R}_{\geq 0}$ and $i \in \mathcal{N}$, and since $t_k^s \leq t_k^r + \varepsilon/4$. This implies $\bar{x} - \underline{x} < 3\varepsilon$, and the claim follows letting $T := T'$.

Suppose next $(r, s) \in \mathcal{E}$. Nodes r and s have at least $3F - 1$ neighbors in common by Assumption 3, so that, by Assumption 1, they have at least $2F - 1$ neighbors in common belonging to $\mathcal{N}$. Since $(r, s) \in \mathcal{E}$, if $s \in \mathcal{D}_r(t_k^r)$ then $\bar{x} - \underline{x} < \varepsilon$. If instead $s \notin \mathcal{D}_r(t_k^r)$ then r can discard at most $F - 1$ of these $2F - 1$ common neighbors as there are no normal nodes with value less than $\underline{x}$. Hence, there are at least F normal nodes belonging to $\mathcal{D}_r(t_k^r) \cap \mathcal{Q}_s$. Following the same reasoning, at t_k^s , if $r \in \mathcal{D}_s(t_k^s)$ then $\bar{x} - \underline{x} < \varepsilon$. Otherwise, node s can discard at most $F - 1$ normal nodes belonging to $\mathcal{D}_r(t_k^r) \cap \mathcal{Q}_s$. Overall, this implies that at least one of these nodes, say node i , must satisfy (17) and the proof follows as before. ■

5. Data acquisition or timing misbehavior

As we are dealing with data acquisition or timing misbehavior, we have $z_i(\cdot) \equiv x_i(\cdot)$ for every $i \in \mathcal{I}$. We will thus only use x_i throughout this section. To prove Theorem 2, we first prove the following result.

Lemma 3. Consider the network system (1)–(7), with the misbehaving nodes exhibiting an error in the operation (i) and/or (iv). Suppose that Assumptions 1 and 2 hold. Let T' be as in Lemma 2, and let r and s be any two nodes belonging to $\mathcal{N}$ such that $x_r(t) = \underline{x}$ and $x_s(t) = \bar{x}$ for all $t \geq T'$. Then, $|\text{ave}_r(t)| < 3\varepsilon/2$ and $|\text{ave}_s(t)| < 3\varepsilon/2$ for all $t \geq T$, where $T := T' + \varepsilon/4$.

Proof. We prove the claim only for node r since the analysis for node s is analogous. Consider any sampling interval T_k^r with $t_k^r \geq$

T' . Notice that $\text{ave}_r(t) \geq 0$ for all $t \in T_k^r$ since by Assumption 1, Lemma 2 and the control logic, $j \in \mathcal{D}_r(t)$ only if $x_j(t) \geq \underline{x}$. We stress that $\mathcal{D}_r(\cdot)$ is defined only for analysis purposes as its computation is done only at the update times. We now determine an upper bound for $\text{ave}_r(\cdot)$ over T_k^r .

Following the same notation as in Section 2.1, let $\mathcal{E}_i(t)$ and $\bar{\mathcal{E}}_i(t)$ be the subset of nodes not belonging to $\mathcal{D}_i(t)$. Decompose $\mathcal{D}_r(t) = \mathcal{A}_r(t) \cup \mathcal{B}_r(t) \cup \mathcal{C}_r(t)$, where

$$\begin{cases} \mathcal{A}_r(t) := \mathcal{D}_r(t) \cap \mathcal{E}_r(t_k^r) \\ \mathcal{B}_r(t) := \mathcal{D}_r(t) \cap \mathcal{D}_r(t_k^r) \\ \mathcal{C}_r(t) := \mathcal{D}_r(t) \cap \bar{\mathcal{E}}_r(t_k^r) \end{cases} \quad (18)$$

This can be done since $i \in \mathcal{D}_r(t)$ only if $i \in \mathcal{Q}_r$ and since $\mathcal{Q}_r = \mathcal{E}_r(t_k^r) \cup \mathcal{D}_r(t_k^r) \cup \bar{\mathcal{E}}_r(t_k^r)$ by construction. The set $\mathcal{C}_r(t)$ consists of the neighborhood of node r that had the highest values at time t_k^r , but have moderate values at t . Decompose $\mathcal{C}_r(t) = \underline{\mathcal{C}}_r(t) \cup \bar{\mathcal{C}}_r(t)$, where

$$\begin{cases} \underline{\mathcal{C}}_r(t) := \{j \in \mathcal{C}_r(t) : x_j(t) = \underline{x}\} \\ \bar{\mathcal{C}}_r(t) := \{j \in \mathcal{C}_r(t) : x_j(t) > \underline{x}\} \end{cases} \quad (19)$$

This can be done since $j \in \mathcal{C}_r(t)$ only if $j \in \mathcal{D}_r(t)$ and $j \in \mathcal{D}_r(t)$ only if $x_j(t) \geq \underline{x}$. We focus on the set $\bar{\mathcal{C}}_r(t)$. Suppose that there are L elements in this set. Obviously $L \leq F$ since $|\bar{\mathcal{E}}_r(t)| \leq F$ for all $t \in \mathbb{R}_{\geq 0}$. Now, to each element of $\bar{\mathcal{C}}_r(t)$ there corresponds at least an element belonging to $\mathcal{Z}_r(t) := \bar{\mathcal{E}}_r(t) \cap (\mathcal{E}_r(t_k^r) \cup \mathcal{D}_r(t_k^r))$, that is $|\mathcal{Z}_r(t)| \geq L$. In other words, if $\bar{\mathcal{C}}_r(t)$ has L nodes, then there must be at least L nodes whose values are more extreme at time t , and those nodes must have come from the set of moderate (or low) values at time t_k^r . In fact, $|\bar{\mathcal{E}}_r(t)| \leq |\bar{\mathcal{E}}_r(t_k^r)| - |\bar{\mathcal{C}}_r(t)| + |\mathcal{Z}_r(t)|$ by construction. Hence, if $|\mathcal{Z}_r(t)| < L$ one has $|\bar{\mathcal{E}}_r(t)| < |\bar{\mathcal{E}}_r(t_k^r)| \leq F$ along with elements in $\mathcal{D}_r(t)$, those belonging to the set $\bar{\mathcal{C}}_r(t)$, which take on a value larger than $\underline{x}$. However, this is not possible by the control logic. Since any element in $\bar{\mathcal{C}}_r(t)$ must take on a value not larger than the value taken on by any element in $\mathcal{Z}_r(t)$, we have

$$\sum_{j \in \mathcal{C}_r(t)} (x_j(t) - \underline{x}) \leq \sum_{j \in \mathcal{Z}_r(t)} (x_j(t) - \underline{x}) \quad (20)$$

As a final step, let $\mathcal{Z}_r(t) = \underline{\mathcal{Z}}_r(t) \cup \bar{\mathcal{Z}}_r(t)$, where

$$\begin{cases} \underline{\mathcal{Z}}_r(t) := \bar{\mathcal{E}}_r(t) \cap \mathcal{E}_r(t_k^r) \\ \bar{\mathcal{Z}}_r(t) := \bar{\mathcal{E}}_r(t) \cap \mathcal{D}_r(t_k^r) \end{cases} \quad (21)$$

Then,

$$\begin{aligned} \sum_{j \in \mathcal{D}_r(t)} (x_j(t) - \underline{x}) &\leq \\ \sum_{j \in (\mathcal{A}_r(t) \cup \underline{\mathcal{Z}}_r(t))} (x_j(t) - \underline{x}) &+ \sum_{j \in (\mathcal{B}_r(t) \cup \bar{\mathcal{Z}}_r(t))} (x_j(t) - \underline{x}) \end{aligned} \quad (22)$$

The first sum on the right side of (22) yields

$$\sum_{j \in (\mathcal{A}_r(t) \cup \underline{\mathcal{Z}}_r(t))} (x_j(t) - \underline{x}) \leq |\mathcal{E}_r(t_k^r)|(t - t_k^r) \quad (23)$$

This follows since $x_j(t) \leq x_j(t_k^r) + t - t_k^r$ for every $j \in \mathcal{I}$ and $t \geq 0$, since $(\mathcal{A}_r(t) \cup \underline{\mathcal{Z}}_r(t)) \subseteq \mathcal{E}_r(t_k^r)$ and because $j \in \mathcal{E}_r(t_k^r)$ only if $x_j(t_k^r) < \underline{x}$. The second sum on the right side of (22) yields

$$\sum_{j \in (\mathcal{B}_r(t) \cup \bar{\mathcal{Z}}_r(t))} (x_j(t) - \underline{x}) \leq \varepsilon + |\mathcal{D}_r(t_k^r)|(t - t_k^r) \quad (24)$$

The last inequality follows since $(\mathcal{B}_r(t) \cup \bar{\mathcal{Z}}_r(t)) \subseteq \mathcal{D}_r(t_k^r)$ and since $\sum_{j \in \mathcal{S}} (x_j(t_k^r) - \underline{x}) < \varepsilon$ for every $\mathcal{S} \subseteq \mathcal{D}_r(t_k^r)$. In fact, $\sum_{j \in \mathcal{D}_r(t_k^r)} (x_j(t_k^r) - \underline{x}) < \varepsilon$ since r stays constant from T' on. Thus,

in order for $\sum_{j \in \mathcal{S}} (x_j(t_k^r) - \underline{x}) \geq \varepsilon$ there should exist at least one node $j \in \mathcal{D}_r(t_k^r) \setminus \mathcal{S}$ such that $x_j(t_k^r) - \underline{x} < 0$. However, since r is the node that attains the minimum value among the normal nodes then $j \in \mathcal{D}_r(t_k^r)$ only if $x_j(t_k^r) \geq \underline{x}$. Overall, we get

$$\sum_{j \in \mathcal{D}_r(t)} (x_j(t) - \underline{x}) \leq \varepsilon + (|\mathcal{E}_r(t_k^r)| + |\mathcal{D}_r(t_k^r)|)(t - t_k^r) < \frac{3}{2}\varepsilon \quad (25)$$

for all $t \in T_k^r$ since $|\mathcal{E}_r(t_k^r)| + |\mathcal{D}_r(t_k^r)| \leq d_r$ and because $t - t_k^r \leq \varepsilon/(4d_r)$ for all $t \in T_k^r$. Finally, since the interval T_k^r is generic, we conclude that $\text{ave}_r(\cdot) < 3\varepsilon/2$ starting from the first update $t_k^r \geq T'$ of node r . Since this occurs not later than $T' + \varepsilon/(4d_r)$, it holds that $\text{ave}_r(t) < 3\varepsilon/2$ for all $t \geq T$. ■

We note that Lemma 3 strongly relies on the fact that there is no control or transmission misbehavior. In fact, in either case, neither (23) nor (24) are valid. We finally proceed with the proof of Theorem 2.

Proof of Theorem 2. Let T be as in Lemma 3, and denote by r and s any two nodes belonging to $\mathcal{N}$ such that $x_r(t) = \underline{x}$ and $x_s(t) = \bar{x}$ for all $t \geq T$. Consider any $t \geq T$. We have

$$\begin{aligned} \text{ave}_s(t) &= \sum_{j \in \mathcal{D}_s(t)} (x_j(t) - \bar{x}) \\ &= \sum_{j \in \mathcal{D}_s(t)} (x_j(t) - \underline{x}) + |\mathcal{D}_s(t)| (\underline{x} - \bar{x}) \end{aligned} \quad (26)$$

Decomposing $\mathcal{D}_s(t) = (\mathcal{D}_s(t) \setminus \mathcal{D}_r(t)) \cup (\mathcal{D}_s(t) \cap \mathcal{D}_r(t))$, the sum term satisfies

$$\sum_{j \in \mathcal{D}_s(t)} (x_j(t) - \underline{x}) < \sum_{j \in (\mathcal{D}_s(t) \setminus \mathcal{D}_r(t))} (x_j(t) - \underline{x}) + \frac{3}{2}\varepsilon \quad (27)$$

which follows from the fact that $\text{ave}_r(t) < 3\varepsilon/2$ in view of Lemma 3, and since $\sum_{j \in \mathcal{S}} (x_j(t) - \underline{x}) < 3\varepsilon/2$ for every $\mathcal{S} \subseteq \mathcal{D}_r(t)$ (cf. the proof of Lemma 3). Hence,

$$\begin{aligned} \text{ave}_s(t) &< \sum_{j \in (\mathcal{D}_s(t) \setminus \mathcal{D}_r(t))} (x_j(t) - \underline{x}) + |\mathcal{D}_s(t)| (\underline{x} - \bar{x}) + \frac{3}{2}\varepsilon \end{aligned} \quad (28)$$

Since s is the node attaining the maximum value among the normal nodes, $j \in \mathcal{D}_s(t)$ only if $x_j(t) \leq \bar{x}$ otherwise it is discarded in view of Assumption 1 and by construction of the control logic. Thus, $x_j(t) \leq \bar{x}$ for all $t \geq T$ and all $j \in \mathcal{D}_s(t)$. Hence,

$$\begin{aligned} \text{ave}_s(t) &< (|\mathcal{D}_s(t) \setminus \mathcal{D}_r(t)| - |\mathcal{D}_s(t)|) (\bar{x} - \underline{x}) + \frac{3}{2}\varepsilon \\ &= -|\mathcal{D}_s(t) \cap \mathcal{D}_r(t)| (\bar{x} - \underline{x}) + \frac{3}{2}\varepsilon \end{aligned} \quad (29)$$

Following the same notation as in Section 2.1, let $\mathcal{E}_i(t)$ and $\bar{\mathcal{E}}_i(t)$ be the set of nodes discarded by $i \in \mathcal{N}$ at time t with associated value smaller than $x_i(t)$ and larger than $x_i(t)$, respectively. For nodes r and s , define

$$\begin{cases} \mathcal{W}_r(t) := \mathcal{E}_r(t) \cap \mathcal{Q}_s \\ \bar{\mathcal{W}}_r(t) := \bar{\mathcal{E}}_r(t) \cap \mathcal{Q}_s \\ \mathcal{W}_s(t) := \mathcal{E}_s(t) \cap \mathcal{Q}_r \\ \bar{\mathcal{W}}_s(t) := \bar{\mathcal{E}}_s(t) \cap \mathcal{Q}_r \end{cases} \quad (30)$$

Fig. 1. Network system considered in the numerical example. Normal nodes are depicted in gray, while the misbehaving node is depicted in orange. The graph satisfies Assumption 3 and is thus robust against generic misbehavior (Theorem 1). The removal of the red edges leads to a graph that satisfies Assumption 4, which is robust against data acquisition or timing misbehavior (Theorem 2). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Thus, at every $t \geq T$, node r discards $|\mathcal{W}_r(t)| + |\bar{\mathcal{W}}_r(t)|$ nodes that are also neighbors of s . Similarly, node s discards $|\mathcal{W}_s(t)| + |\bar{\mathcal{W}}_s(t)|$ nodes that are also neighbors of r . Moreover, $\mathcal{W}_r(t) \subseteq \mathcal{W}_s(t)$ and $\bar{\mathcal{W}}_s(t) \subseteq \bar{\mathcal{W}}_r(t)$. The first relation follows because r is the node attaining the minimum value among the normal nodes. Thus, all the nodes that belong to $\mathcal{W}_r(t)$ take on value less than $\underline{x}$ and hence are necessarily misbehaving. Since these nodes belong to $\mathcal{Q}_s$, they must be all discarded also by node s . In fact, if s discards $L < |\mathcal{W}_r(t)|$ of these nodes then there must exist other $F - L$ nodes in $\mathcal{Q}_s$ but not in $\mathcal{W}_r(t)$ with value less than $\underline{x}$. Since by Lemma 2 there cannot be normal nodes with value less than $\underline{x}$ after T , this would imply that s has at least $F + 1$ misbehaving neighbors contradicting Assumption 1. The same reasoning applies to the relation $\bar{\mathcal{W}}_s(t) \subseteq \bar{\mathcal{W}}_r(t)$. Thus, r and s discard at most $|\mathcal{W}_s(t)| + |\bar{\mathcal{W}}_r(t)| \leq 2F$ neighbors in common.

The proof can be finalized. Suppose first $(r, s) \notin \mathcal{E}$. Since by Assumption 4 nodes r and s have at least $2F + 1$ common neighbors, we have $|\mathcal{D}_s(t) \cap \mathcal{D}_r(t)| \geq 1$. Thus $\text{ave}_s(t) < -(\bar{x} - \underline{x}) + 3\varepsilon/2$. By combining this inequality with $\text{ave}_s(t) > -3\varepsilon/2$ then $\bar{x} - \underline{x} < 3\varepsilon$. Suppose next $(r, s) \in \mathcal{E}$. If $|\mathcal{W}_s(t)| = F$ or $|\bar{\mathcal{W}}_r(t)| = F$ for some t then $\bar{x} - \underline{x} < 3\varepsilon/2$ with no need to resort to (29). For instance, if $|\mathcal{W}_s(t)| = F$ then $r \in \mathcal{D}_s(t)$. Recalling that $\text{ave}_s(t) = \sum_{j \in \mathcal{D}_s(t)} (x_j(t) - \bar{x})$ and that $j \in \mathcal{D}_s(t)$ only if $x_j(t) \leq \bar{x}$, then $\bar{x} - \underline{x} > -3\varepsilon/2$ otherwise we would contradict Lemma 3. If instead $|\mathcal{W}_s(t)| < F$ and $|\bar{\mathcal{W}}_r(t)| < F$ for all t then r and s always discard at most $|\mathcal{W}_s(t)| + |\bar{\mathcal{W}}_r(t)| \leq 2F - 2$ common neighbors. Since by Assumption 4 nodes r and s have at least $2F - 1$ neighbors in common, we have again $|\mathcal{D}_s(t) \cap \mathcal{D}_r(t)| \geq 1$ which gives the claim. ■

6. A numerical example

Consider a network system as in (1)–(7), with $n = 7$ nodes interconnected as in Fig. 1 and $F = 1$ misbehaving node. State and clock initial values are taken randomly within the intervals $[0, 1]$ and $[0, t_{init}]$, respectively, with $t_{init} = 0.15$ s. The desired accuracy level for consensus is selected as $\varepsilon = 0.01$ and we set $\underline{d}_i = \varepsilon/(4d_i)$ for every node. We note that the graph satisfies Assumption 3, which is sufficient to guarantee resilience against generic misbehavior (Theorem 1).

We consider the case of control misbehavior, which is most critical for consensus (cf. Section 2.2). Specifically, we assume that the misbehaving node applies the control input $u_i(t) =$

Fig. 2. Network state evolution with the resilient consensus protocol under control misbehavior. The evolution of the misbehaving node is depicted in red dashed line.

$10 \sin(10\pi t)$ for all $t \in \mathbb{R}_{\geq 0}$ instead of (5). Fig. 2 illustrates the network state evolution with the proposed resilient consensus protocol. In agreement with the conclusions of Theorem 1, one sees that the normal nodes remain in the convex hull containing their initial values and reach a practical agreement disregarding the behavior of the misbehaving node.

7. Conclusions

This paper shows the possibility of approaching the resilient consensus problem in a context where the nodes have their own clocks and can make updates at arbitrary time instants, as in event-triggered and self-triggered control. We considered a scenario where the network supports the data flow with reliability and accuracy, neglecting issues such as data loss, transmission delays and noise. We envision that some extensions in this venue are possible along the same lines as in De Persis and Frasca (2013) and Senejohnny, Tesi, and De Persis (2018) where we discuss aspects related to the quality of the transmission medium.

Our approach utilizes a self-triggered update scheme. It is of interest to investigate if similar results can be obtained also with event-triggered or other types of aperiodic update schemes (Hetel et al., 2017). We also envision an application of this research in the context of distributed optimization (Fazlyab, Nowzari, Pappas, Ribeiro, & Preciado, 2016; Sundaram & Gharesifard, 2015) and coordination with asynchronous cloud access (Nowzari & Pappas, 2016). Also for these problems, self-triggered control represents a viable option to allow for asynchrony without destroying regulation properties. Finally, it is interesting to see how the results of this paper can be extended to Byzantine threat models (LeBlanc et al., 2013) where misbehaving nodes need not send the same value to all of their neighbors at some time instant.

References

- Abbas, W., Vorobeychik, Y., & Koutsoukos, X. (2014). Resilient consensus protocol in the presence of trusted nodes. In *International Symposium on Resilient Control Systems*. IEEE.
- Cao, Y., Yu, W., Ren, W., & Chen, G. (2013). An overview of recent progress in the study of distributed multi-agent coordination. *IEEE Transactions on Industrial Informatics*, 9(1), 427–438.
- Cortés, J. (2006). Finite-time convergent gradient flows with applications to network consensus. *Automatica*, 42(11), 1993–2000.
- De Persis, C., & Frasca, P. (2013). Robust self-triggered coordination with ternary controllers. *IEEE Transactions on Automatic Control*, 58(12), 3024–3038.
- Dibaji, S. M., & Ishii, H. (2015). Consensus of second-order multi-agent systems in the presence of locally bounded faults. *Systems & Control Letters*, 79, 23–29.
- Dibaji, S. M., & Ishii, H. (2017). Resilient consensus of second-order agent networks: Asynchronous update rules with delays. *Automatica*, 81, 123–132.

- Dibaji, S. M., Ishii, H., & Tempo, R. (2018). Resilient randomized quantized consensus. *IEEE Transactions on Automatic Control*, 63(8), 2508–2522.
- Dolev, D., Lynch, N. A., Pinter, S. S., Stark, E. W., & Weihl, W. E. (1986). Reaching approximate agreement in the presence of faults. *Journal of the ACM*, 33(3), 499–516.
- Fazlyab, M., Nowzari, C., Pappas, G. J., Ribeiro, A., & Preciado, V. M. (2016). Self-triggered time-varying convex optimization. In *55th conference on decision and control* (pp. 3090–3097). IEEE.
- Franceschelli, M., Giua, A., & Pisano, A. (2017). Finite-time consensus on the median value with robustness properties. *IEEE Transactions on Automatic Control*, 62(4), 1652–1667.
- Heemels, W. P. M. H., Johansson, K. H., & Tabuada, P. (2012). An introduction to event-triggered and self-triggered control. In *Decision and control (CDC), 2012 IEEE 51st annual conference on* (pp. 3270–3285). IEEE.
- Hetel, L., Fiter, C., Omran, H., Seuret, A., Fridman, E., Richard, J. P., et al. (2017). Recent developments on the stability of systems with aperiodic sampling: An overview. *Automatica*, 76, 309–3350.
- LeBlanc, H. J., & Koutsoukos, X. (2012). Resilient asymptotic consensus in asynchronous robust networks. In *50th annual allerton conference on communication, control, and computing* (pp. 1742–1749). IEEE.
- LeBlanc, H., Zhang, H., Koutsoukos, X., & Sundaram, S. (2013). Resilient asymptotic consensus in robust networks. *IEEE Journal on Selected Areas in Communications*, 31(4), 766–781.
- Lynch, N. A. (1996). *Distributed algorithms*. Morgan Kaufmann.
- Nowzari, C., & Pappas, G. J. (2016). Multi-agent coordination with asynchronous cloud access. In *2016 American control conference* (pp. 4649–4654). IEEE.
- Saldaña, D., Prorok, A., Sundaram, S., Campos, M. F. M., & Kumar, V. (2017). Resilient consensus for time-varying networks of dynamic agents. In *2017 American control conference* (pp. 2378–2386). IEEE.
- Senejohnny, D. M., Tesi, P., & De Persis, C. (2018). A jamming-resilient algorithm for self-triggered network coordination. *IEEE Transactions on Control of Network Systems*, 5, 981–990.
- Sundaram, S., & Gharesifard, B. (2015). Consensus-based distributed optimization with malicious nodes. In *53rd annual allerton conference on communication, control, and computing* (pp. 244–249). IEEE.
- Usevitch, J., & Panagou, D. (2017). r-robustness and (r, s)-robustness of circulant graphs. In *arxiv.org/abs/1710.01990*.
- Vaidya, N. H., Tseng, L., & Liang, G. (2012). Iterative approximate Byzantine consensus in arbitrary directed graphs. In *ACM symposium on principles of distributed computing* (pp. 365–374). IEEE.
- Zhang, H., Fata, E., & Sundaram, S. (2017). A notion of robustness in complex networks. *IEEE Transactions on Control of Network Systems*, 2, 310–320.

Danial M. Senejohnny received the M.Sc. degree in Electrical Engineering, from the Sharif University of Technology, Tehran, Iran, in 2014. He received the Ph.D. degree in Systems & Control from Faculty of Science and Engineering, University of Groningen, the Netherlands, in 2018. He is currently pursuing his career outside academia as Industrial Control Systems Security Consultant. His main research interest is in control theory, and his recent research focuses on cyber-physical systems, resilient control, and information security.

Shreyas Sundaram is an Associate Professor in the School of Electrical and Computer Engineering at Purdue University. He received his MS and Ph.D. degrees in Electrical Engineering from the University of Illinois at Urbana-Champaign in 2005 and 2009, respectively. He was a Postdoctoral Researcher at the University of Pennsylvania from 2009 to 2010, and an Assistant Professor in the Department of Electrical and Computer Engineering at the University of Waterloo from 2010 to 2014. He is a recipient of the NSF CAREER award, and an Air Force Research Lab Summer Faculty Fellowship.

At Purdue, he received the Hesselberth Award for Teaching Excellence and the Ruth and Joel Spira Outstanding Teacher Award. At Waterloo, he received the Department of Electrical and Computer Engineering Research Award and the Faculty of Engineering Distinguished Performance Award. He received the M. E. Van Valkenburg Graduate Research Award and the Robert T. Chien Memorial Award from the University of Illinois, and he was a finalist for the Best Student Paper Award at the 2007 and 2008 American Control Conferences. His research interests include network science, analysis of large-scale dynamical systems, fault-tolerant and secure control, linear system and estimation theory, game theory, and the application of algebraic graph theory to system analysis.

Claudio De Persis is a Professor with the Engineering and Technology Institute, Faculty of Science and Engineering, University of Groningen the Netherlands. He received the Laurea degree in Electronic Engineering in 1996 and the Ph.D. degree in System Engineering in 2000 both from the University of Rome “La Sapienza”, Italy.

Previously he held faculty positions with the Department of Mechanical Automation and Mechatronics, University of Twente and the Department of Computer, Control, and Management Engineering, University of

Rome “La Sapienza”.

He was a Research Associate with the Department of Systems Science and Mathematics, Washington University, St. Louis, MO, USA, in 2000–2001, and with the Department of Electrical Engineering, Yale University, New Haven, CT, USA, in 2001–2002.

His main research interest is in control theory, and his recent research focuses on dynamical networks, cyberphysical systems, smart grids and resilient control. He was an Editor of the *International Journal of Robust and Nonlinear Control* (2006–2013), an Associate Editor of the *IEEE Transactions on Control*

Systems Technology (2010–2015), and of the *IEEE Transactions on Automatic Control* (2012–2015). He is an Associate Editor of *Automatica* (2013–present) and of *IEEE Control Systems Letters* (2017–present).

Pietro Tesi received the Ph.D. degree in Computer & Control Engineering from the University of Florence, Italy, in 2010. He is currently an Assistant Professor at the University of Florence, Italy. He also holds a guest research position at the University of Groningen, The Netherlands. Prior to that, he has been a Research Associate at the University of Genoa, Italy, in 2011–2013, and a Visiting Research Scholar at the University of California at Santa Barbara, CA, USA, in 2008–2009. His main research interests include adaptive and learning systems, hybrid systems and networked control. He is

an Associate Editor of the *IEEE Control Systems Society Conference Editorial Board* (2014–present), and an Editor for the *International Journal of Robust and Nonlinear Control* (2016–present) and the *IEEE Control Systems Letters* (2018–present).