Resilience of coordination networks: data availability and integrity

Mohammadi Senejohnny, Danial

Publication date:
2018

Resilience of Coordination Networks: Data Availability and Integrity

DANIAL M. SENEJOHNNY

The research described in this dissertation has been carried out at the Faculty of Mathematics and Natural Sciences, University of Groningen, the Netherlands.

This dissertation has been completed in partial fulfillment of the requirements of the dutch institute of systems and control (disc) for graduate study.

Cover: Ali bijani

Printed by ProefschriftMaken || www.proefschriftmaken.nl

ISBN 978-94-034-0916-0 (printed version)
ISBN 978-94-034-0915-3 (electronic version)

rijksuniversiteit
groningen

Resilience of Coordination Networks: Data Availability and Integrity

Proefschrift

ter verkrijging van de graad van doctor aan de
Rijksuniversiteit Groningen
op gezag van de
rector magnificus prof. dr. E. Sterken
en volgens besluit van het College voor Promoties.

De openbare verdediging zal plaatsvinden op

vrijdag 30 november 2018 om 11:00 uur

door

Danial Mohammadi Senejohnny

geboren op 18 okt 1988
te Tehran, Iran.

Promotor
Prof. dr. C. De Persis

Copromotor
Dr. P. Tesi

Beoordelingscommissie
Prof. dr. M. Cao
Prof. dr. D. Dimarogonas
Prof. dr. V. Gupta

Acknowledgements

Looking all the way back in time at the very first day that I stepped into Nijenborg 4, I cannot believe how fast my PhD came to an end. Doing PhD at Rijksuniversiteit Groningen and living in this tiny and relatively unknown city in the north of the Netherlands have provided me with unique experience and unforgettable memories that form one of the most pleasant chapters of my life. I would like to thank all the people who played a role in making this chapter.

Firstly, I would like to express my sincere gratitude to my advisor Pietro Tesi for his continuous support during my PhD. His patience, calmness, smartness, and immense knowledge helped me in the course of my research and finalization of this thesis. I would like to appreciate his accessibility, approachability, and all those friendly coffee discussions that we had. I could not have imagined having a better advisor and mentor for my PhD study. I would like to thank my promoter Claudio De Persis for encouraging me to give clearer presentations and setting a higher standard in defining meaningful problems. His research experience was an invaluable asset during my PhD.

I would like to thank my assessment committee for reading my thesis and providing me with their positive and instructive feedback. I am grateful to our support team especially Frederika, for the events, conferences, and gathering that they organized and administrative help that they provided. I would like to briefly recall some nice moments and activities that I shared with my fellow SMSies for which I am grateful: late afternoon squashes with Tobias; Smart grid the game with Eric, Tjardo, and Tobias; footballs with Sebastian and Tjardo; Random discussions with Sebastian when he wanted to take a break and distract others; practicing Farsi greetings with Shuai; asking Mingming about china; FIFA 2015 that we played at office with Erik, Tjardo, and Sebastian when Claudio and Pietro went to Japan for CDC15. I would like to thank Tobias and Erik for accepting to be my paranymphs. I would also like to thank my many current and previous colleagues at SMS, DTPA and JBI for the nice discussion and fun moments that we had during lunch times, at Benelux & CDC conferences, and DISC courses. I am thankful to Ali Bijani for designing my thesis cover pages and invitation in quite a short notice. I am grateful to Café de las lenguas for providing the venue for me and other international people to practicing Dutch in a lively environment and meet new and wonderful people. I would like to thank our small Iranian community especially Hesam and Ahmad Reza for gathering us once a while with different excuses to meet and not to forget our mother tongue Farsi.

Last but not least, I would like to thank my parents and two sisters, Morteza, Fatemeh, Hanieh, and Faezeh for their immense support in the past 4 years. I could not have tolerated being far away from my home, family, and friends without their support.

Danial Mohammadi Senejohnny
Den Haag, The Netherlands
5th Nov 2018

Contents

List of Figures

List of Tables

1 Introduction

Cyber-Physical systems (CPS) are systems where communication, computational and physical devices are interconnected and interact with one another. Such interconnection is brought into practice by integrating Information Technology (IT) and Operational Technology [1] (OT). Cyber-Physical systems bring new opportunities into several industrial and societal domains ranging from transportation and electric power generation to traffic flow management and health care. In fact, CPS are expected to revolutionize all the engineered systems on which our society crucially depends. Internet of Things (IoT), Industry 4.0, Smart Cities, and Smart Grid, are all concepts revolving around Cyber-Physical systems.

Many of the above mentioned sectors and industries are critical infrastructure, in the sense that they are essential to the health, safety, and security of our society. This emphasizes the importance of rendering CPS "resilient" against malfunctioning due to genuine failures or cyberattacks. An example of a cyberattack affecting CPS is Stuxnet. Stuxnet invaded Iranian uranium enrichment facilities in 2010, and this is widely regarded as the first major CPS attack. In 2014, German steel mill blast furnace was destroyed after hackers gained access of German company computers. Late 2015 and 2016, Ukrainian electricity network experienced a power outage as a result of the cyberattack compromising the electricity distribution infrastructure. In all the aforementioned examples, the Malware was designed to attack industrial control systems.

Currently, the dominant look at control system security is from computer science and IT perspectives which focus mostly on prevention mechanisms (Knapp and Langill, 2011; Knapp and Samani, 2013; Radvanovsky and Brodsky, 2016; Macaulay, 2016; Macaulay and Singer, 2016). This perspective revolves around concepts like firewalls, network segmentation, and access control. This approach provides the first layer of protection for the security of control systems. However, it is not sufficient and fails to address how, and to what extent a control system can continue to operate in case an attack turns

[1] Operational Technology (OT) is the hardware and software dedicated to control and monitoring of physical processes. Few examples include: PLC's, SCADA, DCS.

out to be successful. This triggers the necessity of introducing the concept of *resilient* control as an extra layer of protection. The main objective of this thesis is to address this problem.

1.1 SELF-TRIGGERED COORDINATION

Cyber-physical systems feature a paradigm shift from centralized to distributed control and computation. In this thesis, we will address the question of designing resilient control protocols for CPS with respect to consensus and synchronization problems. *Consensus* is a prototypical problem in distributed settings with an enormous range of applications, spanning from formation and cooperative robotics to surveillance and distributed computing; see for instance Bai et al. (2011); Olfati-Saber and Murray (2004). The terms consensus and coordination are used interchangeably throughout the thesis. In this thesis we will mostly focus on consensus problems, although some results will be discussed also in connection with the problem of synchronizing linear oscillators. We will address the problem of reaching resilient coordination in a context where the nodes have their own clocks, possibly operating in an *asynchronous* way, and can make updates at arbitrary time instants. Besides the practical difficulties in achieving a perfect clock synchronization, one main reason for considering independent clocks is related to developments in the area of networked control systems where, in order to enhance energy efficiency and flexibility, it is more and more required to have fully autonomous devices, which is the paradigm of *event-triggered* and *self-triggered* control (Heemels et al., 2012; Hetel et al., 2017; Dimarogonas et al., 2012; Postoyan et al., 2015; De Persis and Postoyan, 2017; Nowzari et al., 2017). In fact, our approach utilizes self-triggered coordination protocols inspired by De Persis and Frasca (2013). Each node is equipped with a clock that determines when the next update is scheduled. At the update instant, the node polls its neighbors, collects the data and determines whether it is necessary to modify its controls along with a bound on the next update instant.

1.2 RESILIENCE AGAINST DATA AVAILABILITY AND INTEGRITY ATTACKS

In this thesis we will investigate the problem of designing resilient control protocols for CPS with respect to the questions of data availability and integrity.

The first question is related to to the fact that data flow can be occasionally interrupted, while the second question is related to the fact that the data content might be corrupted. This is motivated by the following considerations. The difference between IT and OT security is not just confined to the extent of attack impact but also requires the right risk assessments strategy to prioritize security parameters. The traditional information security CIA triad *Confidentiality*, *Integrity*, and *Availability* also applies to OT networks (Cardenas et al., 2008), but not at the same order as IT networks. In IT networks the order of importance is represented by C-I-A. In OT networks, however, the focus is not on information but on the industrial process. Therefore, real-time availability of data is the most crucial factor to ensure normal operation of the system. As the second factor, integrity is also important, since misrepresentation of data results in undesired decision or control action. Confidentiality usually has a lower priority in industrial control systems. This changes the order of importance to A-I-C for OT networks and influences the representation of the content of this thesis.

In the CPS literature attacks to the communication links are classified as either Denial-of-Service (DoS) or deception attacks (Sandberg et al., 2015; Amin et al., 2009). These attacks are representative of data Availability and Integrity attacks, respectively. The former affect the timeliness of information exchange, *i.e.*, to cause packet loss. Part I is concerned with DoS attacks and, in particular, *jamming* attacks (Xu et al., 2006; Thuente and Acharya, 2006), although we shall use these two terms interchangeably. We will mostly refer to jamming attacks since this is one of the main sources of communication interruption in wireless sensor networks, which represent the most important application domains of our study. Deception attacks are instead primarily intended to affect the trustworthiness of data by manipulating the packets transmitted over the network; see Fawzi et al. (2011, 2014); Pasqualetti et al. (2015); Teixeira et al. (2015a); Bai et al. (2017); Smith (2015); Mo et al. (2015); Mo and Sinopoli (2016); Zhu and Martínez (2014); LeBlanc et al. (2013) and the references therein. Part II is concerned with Deception attacks. In this thesis, we will focus on the problem of designing resilient control protocols. A parallel research line focuses on the problem of detecting attacks (Shi et al., 2018; Bai et al., 2015). This is a very important research line that should be regarded as complementary to the present one. A detail account of the thesis outline is in order.

1.3 OUTLINE OF THE THESIS

This thesis consists of two main parts, each studying a particular type of security issue that can affect cyber-physical systems performance. Both parts have a separate introduction, statement of contributions and a more detailed outline.

Part I pertains to Data Availability Attacks. All the three chapters consider the absence of data and information accessibility due to genuine failure or cyberattacks, which results in Denial-of-Service (DoS). However, in particular we are concerned with *jamming* attacks as we are mainly interested in wireless sensor networks. In chapter 2 we consider a shared communication network, i.e. "infrastructure" mode, which is compromised by a jamming attack. Then we propose a resilient protocol that ensures coordination in spite of the presence of such attacks/malfunctions. The results are extended to "ad-hoc" peer-to-peer communication network in chapter 3. While chapter 2 and 3 deal with single integrator networks, chapter 4 extends the analysis to higher-order dynamical systems, which is relevant to deal with network synchronization problems.

Part II pertains to Data Integrity Attacks. The presence of unreliable information in the network could be as a result of genuine fault in the system or cyberattack. Chapter 5 investigates the resilient consensus protocol against several types of node misbehavior resulting from error in operations such as data acquisition, data transmission, control logic, and update time scheduler. In chapter 6, inspired by De Persis and Frasca (2013), we use a different coordination protocol aimed at relaxing the graph connectivity condition in chapter 5.

After Part II, we provide some summarizing remarks and suggestions for future research.

1.4 LIST OF PUBLICATIONS

1.4.1 JOURNAL PUBLICATIONS

- D. Senejohnny, P. Tesi, and C. De Persis, "A jamming-resilient algorithm for self-triggered network coordination," *IEEE Transactions on Control of Network Systems, In Press*, 2017 (Chapter 3).

- D. Senejohnny, S. Sundaram, C. De Persis, and P. Tesi, "Resilience against misbehaving nodes in asynchronous networks," *Automatica, Provisionally accepted as Brief Paper*, 2018 (Chapter 5).

- D. Senejohnny, S. Sundaram, C. De Persis, and P. Tesi, "Misbehavior-resilient asymptotic coordination in asynchronous networks," *Under Prepration*, 2018 (Chapter 6).

1.4.2 BOOK CHAPTERS

- D. Senejohnny, P. Tesi, and C. De Persis, "Resilient self-triggered network synchronization," in *Control Subject to Computational and Communication Constraints*, S. Tarbouriech, A. Girard, and L. Hetel, Eds. Springer International Publishing, 2018, ch. 11 (Chapter 4).

1.4.3 CONFERENCE PUBLICATIONS

- D. Senejohnny, P. Tesi, and C. De Persis, "Self-triggered coordination over a shared network under denial-of-service," in *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*. IEEE, 2015, pp. 3469–3474 (Chapter 2).

- D. Senejohnny, P. Tesi, and C. De Persis, "Resilient self-triggered network synchronization," in *Decision and Control (CDC), 2016 IEEE 55th Conference on*. IEEE, 2016, pp. 489–494 (Chapter 4).

- D. Senejohnny, S. Sundaram, C. De Persis, and P. Tesi, "Resilience against misbehaving nodes in self-triggered networks," in *Decision and Control (CDC), 2018 IEEE 57th Conference on*. IEEE, 2018 (Chapter 5).

1.4.4 BENELUX CONFERENCE ABSTRACTS

- D. Senejohnny, P. Tesi, and C. De Persis, "Denial of Service in Distributed Control and Communication Systems", 34^{th} Benelux Meeting on Systems and Control, March 2015, Lommel, Belgium.
- D. Senejohnny, P. Tesi, and C. De Persis, "Self-triggered Coordination over a Shared Network under Denial-of-Service", 35^{th} Benelux Meeting on Systems and Control, Soesterberg, The Netherlands.
- D. Senejohnny, P. Tesi, and C. De Persis, "Resilient Self-triggered Network Synchronization", 36^{th} Benelux Meeting on Systems and Control, Spa, Belgium.
- D. Senejohnny, S. Sundaram, C. De Persis, and P. Tesi, " Resilience against Misbehaving Nodes in Asynchronous Networks", 37^{th} Benelux Meeting on Systems and Control, Soesterberg, The Netherlands.

1.5 NOTATIONS

The notation adopted in this thesis is in the main standard. We denote by $\mathbb{R}$, $\mathbb{R}_{>0}$, $\mathbb{R}_{\geq 0}$ the sets of real, positive, and nonnegative numbers, respectively. Also, we denote by $\mathbb{Z}_{\geq 0}$ the set of nonnegative integers. The rest of the widely used notations used throughout the thesis are summarized in Table 1.1. In this table, i and ij mainly refer to nodes and edges. Furthermore, superscripts represent vector and subscripts represents scalar nature of the state variables.

Table 1.1: Some of the symbols and parameters widely used in the thesis

	State variables
$x_i \in \mathbb{R}$, $x^i \in \mathbb{R}^n$	state variable of node *i*
$\theta_i \in \mathbb{R}$, $\theta^{ij} \in \mathbb{R}^n$	local clock variable of node and edge *ij*
$u_i \in \mathbb{R}$, $u^i \in \mathbb{R}^n$	control variable of node *i*
$u_{ij} \in \mathbb{R}$, $\xi^{ij} \in \mathbb{R}^n$	control variable of edge *ij*
$\eta^i \in \mathbb{R}^n$	control state variable of node *i*
	Controller
ε	Sensitivity Parameter
t^i_k, t^{ij}_k	*k*-th update time at node *i* and edge *ij*
d^i	degree of node *i*
	Denial-of-Service (DoS)
h_n, h^{ij}_n	Sequence of DoS on/off transitions
τ_n, τ^{ij}_n	length of DoS
H_n, H^{ij}_n	*n*-th DoS time-interval
Ξ, Ξ^{ij}	set of time instances where communication is denied
Θ, Θ^{ij}	set of time instances where communication is allowed
	Sets
$\mathcal{G}$	Undirected connected graph
$\mathcal{I}$	The set of nodes of $\mathcal{G}$
$\mathcal{E}$	The set of edges of $\mathcal{G}$
$\mathcal{L}$	Laplacian matrix of $\mathcal{G}$
$\mathcal{B}$	Incidence matrix of $\mathcal{G}$
$\mathcal{Q}_i$	The set of neighbors of node *i*

PART I

Data Availability Attack

Introduction

Wireless sensor networks are an important component in CPS. However, they are less reliable than wired networks and more prone to genuine and malicious disconnections. Jamming causes Denial-of-Service (DoS) phenomena and is defined as the disruption of existing wireless communication between sender and receiver so that no information packet can be exchanged. As the result of jamming the signal-to-noise ratio at the receiver's side is decreased. The nature of jamming can be due to either unintentional (genuine) interference caused in the communication or intentional (malicious) interference by an attacker with the aim of hindering or distorting communicated packets.

In the literature, the issues of securing robustness of CPS against DoS has been widely investigated only for centralized architectures (Amin et al., 2009; Gupta et al., 2010; Befekadu et al., 2011; Teixeira et al., 2015b; Foroush and Martinez, 2012; De Persis and Tesi, 2014, 2015; Cetinkaya et al., 2017, 2018a; De Persis and Tesi, 2016). On the other hand, very little is known about DoS for distributed coordination problems. In this part, we investigate the issue of DoS, genuine failure or cyberattack, with respect to consensus-like networks. The attacker's objective is to prevent consensus by denying communication among the network agents.

A basic question in the analysis of distributed coordination in the presence of DoS is concerned with the modeling of DoS attacks. In De Persis and Tesi (2014, 2015, 2018), a general model is considered that only constrains DoS attacks in terms of their average frequency and duration, which makes it possible to capture many different types of DoS attacks, including trivial, periodic, random and protocol-aware jamming attacks (Thuente and Acharya, 2006; Xu et al., 2005; Tague et al., 2009). This model is also employed in different settings (Dolk et al., 2017; Cetinkaya et al., 2018b,a; Lu and Yang, 2018)

OUTLINE AND CONTRIBUTION

Building on De Persis and Tesi (2015), a preliminary analysis of consensus networks in the presence of DoS is presented in chapter 2 under the simplifying assumption that the occurrence of DoS causes all the network links to fail simultaneously. This scenario is representative of networks operating through a single access point, in the so-called "infrastructure" mode. In chapter 3 and 4, we consider the more general scenario in which the network communication links can fail independent of each other, thereby extending the analysis to "ad-hoc" (peer-to-peer) networks.

The main contribution of Part I is an explicit characterization of the frequency and duration of DoS for both infrastructure mode and peer-to-peer (P2P) networks under which consensus can be preserved by suitably designing time-varying control and communication policies. We also provide an explicit characterization of the effects of DoS on the consensus time and show that the considered analysis framework is general enough to account as well for "genuine" DoS, *i.e.*, for natural network congestion phenomena. Finally, chapter 2 and 3 consider resilient consensus in a network of single integrator dynamical systems, while chapter 4 investigates resilient synchronization in a network of higher-order dynamical systems.

In a technical sense, since DoS induces communication failures, the problem of achieving consensus under DoS can be naturally cast as a consensus problem for networks with switching topologies. This approach is certainly not new in the literature. In Olfati-Saber and Murray (2004), for instance, it is shown that consensus can be reached whenever graph connectivity is preserved point-wise in time; Arcak (2007) considers a notion of *Persistency-of-Excitation* (PoE), which stipulates that graph connectivity should be established over a period of time, rather than point-wise in time, which is similar to the joint connectivity assumption in Jadbabaie et al. (2003). In CPS, however, the situation is different. In CPS, one needs to deal with the fact that networked communication is inherently digital, which means that the rate at which the transmissions are scheduled cannot be arbitrarily large. Under such circumstances, the aforementioned tools turn out to be ineffective. In order to cope with this situation, in this chapter we introduce a notion of *Persistency-of-Communication* (PoC), which naturally extends the PoE condition to a digital networked setting by requiring graph (link) connectivity over periods of time that are consistent with the constraints imposed by the communication medium. A characterization of DoS frequency and duration under which consensus properties are preserved is then obtained by exploiting the PoC condition.

2

Jamming-resilient Coordination over Shared Networks

ABSTRACT

The issue of cyber-security has become ever more prevalent in the analysis and design of cyber-physical systems. In this chapter, we investigate self-triggered consensus networks in the presence of communication failures caused by Denial-of-Service (DoS) attack, namely attacks that prevent communication among the network agents simultaneously. By introducing a notion of Persistency-of-Communication (PoC), we provide a characterization of DoS frequency and duration such that consensus is not destroyed. An example is given to substantiate the analysis.

Published as:

D. Senejohnny, P. Tesi, and C. De Persis, "Self-triggered coordination over a shared network under denial-of-service," in *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*. IEEE, 2015, pp. 3469–3474.

2.1 PROBLEM FORMULATION

2.1.1 DISTRIBUTED CONTROL SYSTEM

We assume to have a set of nodes $\mathcal{I} = \{1, \dots, n\}$ representing our agents and an undirected connected graph $\mathcal{G} = (\mathcal{I}, \mathcal{E})$ with $\mathcal{E}$ a set of unordered pairs of nodes, called edges. We denote by $\mathcal{B}$ and $\mathcal{L}$ the Incidence and Laplacian matrix of $\mathcal{G}$, respectively, where the latter is a symmetric matrix. For each node $i \in \mathcal{I}$, we denote by $\mathcal{Q}_i$ the set of its neighbors, and by d^i its degree, that is, the cardinality of $\mathcal{Q}_i$.

We consider the following hybrid dynamics on a triplet of n-dimensional variables involving the consensus variable x, the controls u, and the local clock variables θ. All these variables are defined for time $t \geq 0$. Controls are assumed to belong to $\{-1, 0, +1\}$. The specific quantizer of choice is $\operatorname{sign}_\varepsilon : \mathbb{R} \to \{-1, 0, +1\}$, defined according to

$$\operatorname{sign}_\varepsilon(z) = \begin{cases} \operatorname{sign}(z) & \text{if } |z| \geq \varepsilon \\ 0 & \text{otherwise} \end{cases} \tag{2.1}$$

where $\varepsilon > 0$ is a sensitivity parameter, which can be used at the design stage for trading-off frequency of the control updates vs. accuracy of the consensus region.

The system $(x, u, \theta) \in \mathbb{R}^{3n}$ in the *nominal operating mode*, *i.e.*, in the absence of DoS, satisfies the following continuous evolution

$$\begin{cases} \dot{x}_i = u_i \\ \dot{u}_i = 0 \\ \dot{\theta}_i = -1 \end{cases} \tag{2.2}$$

except for every t such that the set

$$\mathcal{S}(\theta, t) = \{i \in \mathcal{I} \ : \ \theta_i(t^-) = 0\}$$

is non-empty, where $s(t^-)$ denotes the limit from below of a signal $s(t)$, *i.e.*, $s(t^-) = \lim_{\tau \nearrow t} s(\tau)$. At such time instants, the system satisfies the following discrete evolution

$$\begin{cases} x_i(t) = x_i(t^-) \quad \forall\, i \in \mathcal{I} \\ u_i(t) = \begin{cases} \mathrm{sign}_\varepsilon(\mathrm{ave}_i(t)) & \text{if } i \in \mathcal{S}(\theta, t) \\ u_i(t^-) & \text{otherwise} \end{cases} \\ \theta_i(t) = \begin{cases} f_i(x(t)) & \text{if } i \in \mathcal{S}(\theta, t) \\ \theta_i(t^-) & \text{otherwise} \end{cases} \end{cases} \tag{2.3}$$

where for every $i \in \mathcal{I}$ the map $f_i : \mathbb{R}^n \to \mathbb{R}_{>0}$ is defined by

$$f_i(x(t)) = \begin{cases} \dfrac{|\,\mathrm{ave}_i(t)|}{4d^i} & \text{if} \quad |\,\mathrm{ave}_i(t)| \geq \varepsilon \\ \dfrac{\varepsilon}{4d^i} & \text{if} \quad |\,\mathrm{ave}_i(t)| < \varepsilon \end{cases} \tag{2.4}$$

where, for conciseness, we have defined

$$\mathrm{ave}_i(t) = \sum_{j \in \mathcal{Q}_i} (x_j(t) - x_i(t)) \tag{2.5}$$

Self-triggered coordination algorithms such as (2.2)-(2.4). turn out to be of major interest when consensus has to be achieved in spite of possibly severe communication constraints. In this respect, a remarkable feature of self-triggered coordination lies in the possibility of ensuring consensus properties in the absence of any global information on the graph topology and with no need to synchronize the agents local clocks De Persis and Frasca (2013).

The result which follows characterizes the convergence properties of (2.2)-(2.4) in the nominal operating mode, and will serve as a basis for the developments of the paper.

Theorem 2.1. *De Persis and Frasca (2013). Given any $\bar{x} \in \mathbb{R}^n$, let $x(t)$ be the solution to* (2.2)-(2.4) *with $x(0) = \bar{x}$. Then $x(t)$ converges in finite time to a point $x^* \in \mathbb{R}^n$ belonging to the set*

$$\mathcal{E} = \{x \in \mathbb{R}^n \ : \ |\sum_{j \in \mathcal{Q}_i} (x_j - x_i)| < \varepsilon \ \forall\, i \in I\} \tag{2.6}$$

2.1.2 DENIAL-OF-SERVICE

We shall refer to DoS as the phenomenon by which communication across the network is not possible. More specifically, we assume that the network nodes make use of a shared communication medium. Under DoS, none of the network nodes can send or receive information. This scenario is representative of several possible DoS threats. In order to maintain continuity, a discussion on this point is deferred to Section 2.1.3. Here, we proceed with the DoS modeling and introduce a number of assumption on its frequency and duration.

Let $\{h_n\}_{n \in \mathbb{Z}_{\geq 0}}$, where $h_0 \geq 0$, denote the sequence of DoS off/on transitions, *i.e.*, the time instants at which DoS exhibits a transition from zero (communication is possible) to one (communication is interrupted). Then

$$H_n := \{h_n\} \cup [h_n, h_n + \tau_n[\tag{2.7}$$

represents the n-th DoS time-interval, of a length $\tau_n \in \mathbb{R}_{>0}$, over which communication is not possible. Here and in the sequel, it is understood that $h_{n+1} > h_n + \tau_n$ for all $n \in \mathbb{Z}_{\geq 0}$, otherwise $H_n \cup H_{n+1}$ could be regarded as a single DoS interval.

Given $t, \tau \in \mathbb{R} \geq 0$, with $t \geq \tau$, let

$$\Xi(\tau, t) := \bigcup_{n \in \mathbb{Z}_{\geq 0}} H_n \bigcap [\tau, t] \tag{2.8}$$

represent the sets of time instants where communication is denied and

$$\Theta(\tau, t) := [\tau, t] \setminus \Xi(\tau, t) \tag{2.9}$$

represent the sets of time instants where communication is allowed, where $\setminus$ denote the relative complement.

In connection with the definition of the DoS sequence in (2.7), the first question to be addressed is that of determining the amount of DoS that the network can tolerate before consensus, as defined in Theorem 2.1, is lost. In this respect, it is simple to see that such an amount is not arbitrary, and that suitable conditions must be imposed on both DoS frequency and duration.

Let us first consider the frequency at which DoS can occur. First notice that $\varepsilon/4d^i$ provides a lower bound on the inter-sampling rate of the i-th node of the network, as imposed by the communication medium. Let now $\Lambda_n = h_{n+1} - h_n$, with $n \in \mathbb{Z}_{\geq 0}$, denote the time elapsing between any two successive DoS triggering. By letting $d_{min} = \min_{i \in I} d^i$, one immediately sees that if

$$\Lambda_n \leq \Delta_* := \frac{\varepsilon}{4d_{min}}$$

then consensus could be destroyed irrespective of the adopted communication strategy. This is because DoS would be allowed to occur at a rate faster than or equal to the sampling rate of some network node, which would clearly preclude the possibility to achieve consensus. It is intuitively clear that, in order to get stability, the frequency at which DoS can occur must be sufficiently small compared to sampling rate of the network nodes. A natural way to express this requirement is via the concept of average dwell-time, as introduced by Hespanha and Morse (1999). Given $t, \tau \in \mathbb{R} \geq 0$ with $t \geq \tau$, let $n(\tau, t)$ denote the number of DoS off/on transitions occurring on the interval $[\tau, t[$.

Assumption 2.1 (DoS frequency). *There exist $\mu \in \mathbb{R}_{\geq 0}$ and $\tau_f \in \mathbb{R}_{>\Delta_*}$ such that*

$$n(\tau, t) \leq \mu + \frac{t - \tau}{\tau_f} \tag{2.10}$$

for all t, $\tau \in \mathbb{R}_{\geq 0}$ and $t \geq \tau$.

In addition to the DoS frequency, one also need to enforce constraints on the DoS duration, namely the length of the intervals over which communication is interrupted. To see this, consider for example a DoS sequence consisting of the singleton $\{h_0\}$. Assumption 2.1 is clearly satisfied with $\mu \geq 1$. However, if $H_0 = \mathbb{R}_{\geq 0}$ (communication is never possible) then stability is lost regardless of the adopted control update policy. Recalling the definition of the set Ξ in (2.8), the assumption that follows provides a quite natural counterpart of Assumption 2.1 with respect to the DoS duration.

Assumption 2.2 (DoS Duration). *There exist $\kappa \in \mathbb{R}_{\geq 0}$ and $\tau_d \in \mathbb{R}_{>1}$such that*

$$|\Xi(\tau, t)| \leq \kappa + \frac{t - \tau}{\tau_d} \tag{2.11}$$

for all t, $\tau \in \mathbb{R}_{\geq 0}$ and $t \geq \tau$.

In words, Assumption 2.2 expresses the property that, on average, the time instances over which communication is denied do not exceed a certain fraction of time, as specified by $\tau_d \in \mathbb{R}_{>1}$.

2.1.3 DISCUSSION

The considered assumptions only constrains the attacker action in time by posing limitations on the frequency of DoS and its duration. Such a characterization can capture many different scenarios, including trivial, periodic, random and protocol-aware jamming attacks Thuente and Acharya (2006)Xu et al. (2005)DeBruhl and Tague (2011) Tague et al. (2009). For the sake of simplicity, we limit out discussion to the case of radio frequency (RF) jammers, although similar considerations can be made with respect to spoofing-like threats Bellardo and Savage (2003).

Consider for instance the case of *constant jamming*. Constant jamming is one of the most common threats that may occur in a wireless network Pelechrinis et al. (2011); Xu et al. (2006). By continuously emitting RF signals on the wireless medium, this type of jammer can lower the Packet Send Ratio (PSR) for transmitters employing carrier sensing as medium access policy as well as lower the Packet Delivery Ratio (PDR) by corrupting packets at the receiver. In general, the percentage of packet losses caused by this type of jammer depends on the Jamming-to-Signal Ratio and can be difficult to quantify as it depends, among many things, on the type of anti-jamming devices, the possibility to adapt the signal strength threshold for carrier sensing, and the interference signal power, which may vary with time. In fact, there are several provisions that can be taken in order to *mitigate* DoS attacks, including spreading techniques, high-pass filtering and encoding DeBruhl and Tague (2011); Tague et al. (2009). These provisions decrease the chance that a DoS attack will be successful, and, as such, limit in practice the frequency and duration of the time intervals over which communication is effectively denied. This scenario can be nicely described via Assumption 2.1 and 2.2.

As another example, consider the case of *reactive jamming* Xu et al. (2006); Pelechrinis et al. (2011). By exploiting the knowledge of the 802.1i MAC layer protocols, a jammer may restrict the RF signal to the packet transmissions. The collision period need not be long since with many CRC error checks a single bit error can corrupt an entire frame. Accordingly, jamming takes the form of a (high-power) burst of noise, whose duration is determined by the length of the symbols to corrupt DeBruhl and Tague (2011); Wood and Stankovic (2002). Also this case can be nicely accounted for via the considered assumptions.

2.2 MAIN RESULT

In section 2.2.1 we introduce a modified consensus protocol to account for the presence DoS, and we present the main result of the paper. The proofs are reported in section 2.2.2.

2.2.1 MODIFIED CONSENSUS PROTOCOL

The consensus protocol in (2.3) needs to be modified in order to achieve robustness against DoS. In this respect, for every t such that the set $\mathcal{S}(\theta, t) = \{i \in \mathcal{I} \ : \ \theta_i(t^-) = 0\}$ is not nonempty, the nominal discrete evolution is modified as follows:

$$\begin{cases} x_i(t) = x_i(t^-) \quad \forall\, i \in \mathcal{I} \\ u_i(t) = \begin{cases} \operatorname{sign}_\varepsilon(\operatorname{ave}_i(t)) & \text{if } i \in \mathcal{S}(\theta,t) \wedge t \in \Theta(0,t) \\ 0 & \text{if } i \in \mathcal{S}(\theta,t) \wedge t \in \Xi(0,t) \\ u_i(t^-) & \quad \text{otherwise} \end{cases} \\ \theta_i(t^+) = \begin{cases} f_i(x(t)) & \text{if } i \in \mathcal{S}(\theta,t) \wedge t \in \Theta(0,t) \\ \frac{\varepsilon}{4d^i} & \text{if } i \in \mathcal{S}(\theta,t) \wedge t \in \Xi(0,t) \\ \theta_i(^-) & \quad \text{otherwise} \end{cases} \end{cases} \tag{2.12}$$

In words, when a network node attempts to communicate and communication is denied, the control signal is set to zero until the subsequent attempt [1].

To implement the consensus protocol nodes rely on their local clocks θ_i. The jump times of each variable θ_i naturally define a sequence of local switching times, which we denote by $\{t_k^i\}_{k \in \mathbb{Z}_{\geq 0}}$. In particular, we have

$$t_{k+1}^i = t_k^i + \begin{cases} f_i(x(t_k^i)) & t_k^i \in \Theta(0,t) \\ \dfrac{\varepsilon}{4d^i} & \quad t_k^i \in \Xi(0,t) \end{cases} \qquad \forall\, i \in \mathcal{I}. \tag{2.13}$$

The modified algorithm basically consists of a two-mode sampling logic. As it will become clear later on, this is in order to maximize the robustness of the

[1] It is worth noting that this implicitly requires that the nodes be able to detect the DoS status. This is the case, for instance, when jamming causes the channel to be busy. Then, transmitters employing carrier sensing as medium access policy can detect the DoS status. Another example is when transceivers employ TCP acknowledgment.

consensus protocol against DoS. By (2.13), it is an easy matter to see that the sequences of local switching times $\{t_k^i\}_{k \in \mathbb{Z}_{\geq 0}}$ satisfy a "dwell time" property since

$$\Delta_k^i := t_{k+1}^i - t_k^i \geq \frac{\varepsilon}{4 d_{\max}}. \tag{2.14}$$

for every $i \in \mathcal{I}$ and $k \geq 0$, where $d_{max} = \max_{i \in I} d^i$.

For the sake of clarity, the modified consensus protocol is summarized below.

Modified Consensus Protocol (for each $i \in \mathcal{I}$)

```
initialization: set $u_i(0) \in \{-1, 0, +1\}$ and $\theta_i(0) = 0$;
while $\theta_i(t) > 0$ do
    $i$ applies the control $u_i(t)$;
end while
if $\theta_i(t^-) = 0$ & $t \in \Theta(0, t)$ then
    for all $j \in \mathcal{Q}_i$ do
        $i$ polls $j$ and collects the information $x_j(t) - x_i(t)$;
    end for
    $i$ computes $\mathrm{ave}_i(t)$;
    $i$ computes $\theta_i(t)$ as in (2.12);
    $i$ computes $u_i(t)$ as in (2.12);
else
    if $\theta_i(t^-) = 0$ & $t \in \Xi(0, t)$ then
        $i$ set $u_i(t) = 0$;
        $i$ set $\theta_i(t) = \frac{\varepsilon}{4 d^i}$;
    end if
end if
```

We are now in position to characterize the overall network behavior in the presence of DoS. In this respect, the analysis is subdivided into two main steps: i) we first prove that regardless of the DoS all the network nodes eventually stop to update their local controls; and ii) we then provide conditions on the DoS frequency and duration under which consensus, in the sense of (2.6), is preserved. This is achieved by resorting to a notion of *Persistency-of-Communication* (PoC), which stipulates that disruptions of the graph connectivity cannot exceed a prescribed threshold.

As for ii), the following result holds true. To maintain continuity, the proof of the results of this section are postponed to section 2.2.2.

Proposition 2.1. (Convergence of the solutions) *Let $x(t)$ be the solution to* (2.2) *and* (2.12). *Then, for every initial condition $x(0)$, there exists a finite time T_1 such that $u_i(t) = 0$ for all $t > T_1$ and $i \in \mathcal{I}$.*

By proposition 2.1, all the controls are set to zero after a finite time T_1. Moreover, after T_1each node tries to sample and transmit periodically with period $\varepsilon/4d^i$. If consensus, in the sense of (2.6), is not achieved this necessarily means that for some node $i \in \mathcal{I}$ all the communication attempts are destroyed. Let

$$\begin{aligned} \bar{\Xi}(\tau, t) &:= \bigcup_{n \in \mathbb{Z}_{\geq 0}} \bar{H}_n \bigcap [\tau, t] && (2.15) \\ \bar{\Theta}(\tau, t) &:= [\tau, t] \setminus \bar{\Xi}(\tau, t) && (2.16) \end{aligned}$$

where

$$\bar{H}_n := \{h_n\} \cup [h_n, h_n + \tau_n + \Delta_* [$$

By the above arguments, a sufficient condition under which communication is not persistently destroyed is that for any τ there exist a t such that $\bar{\Theta}(\tau, t)$ has positive measure. This is because if the above property is true, then $[\tau, t[$ contains a DoS-free interval of length grater than Δ_*, which is grater than $\varepsilon/4d^i$ for every $i \in \mathcal{I}$. The following result then holds.

Proposition 2.2. (Persistency-of-Communication) *Let $x(t)$ be the solution to* (2.2) *and* (2.12). *Consider any DoS sequence satisfying Assumption 2.1 and 2.2 with*

$$\varphi(\tau_f, \tau_d, \Delta_*) := \frac{1}{\tau_d} + \frac{\Delta_*}{\tau_f} < 1 \qquad (2.17)$$

and μ and κ arbitrary. Then, for every τ, the set $\bar{\Theta}(\tau, t)$ has positive measure for any time t satisfying

$$t > \tau + \frac{\kappa + (1 + \mu)\Delta_*}{1 - \varphi(\tau_f, \tau_d, \Delta_*)} \qquad (2.18)$$

Combining Proposition 2.1 and 2.2, the main result of this chapter follows at once.

Theorem 2.2. *Let $x(t)$ be the solution to* (2.2) *and* (2.12)*. Consider any DoS sequence that satisfies Assumption 2.1 and 2.2 with τ_f and τ_d as in (2.17) and μ and κ arbitrary. Then, for every initial condition, $x(t)$ converges in finite time to a point x^* belonging to the set $\mathcal{E}$ as in (2.6).*

Remark 2.1. Condition (2.17) in Proposition 2.2 amounts to requiring that the DoS signal does not destroy communication in a persistent way. This requirement is indeed reminiscent of *Persistency-of-Excitation* (PoE) conditions that are found in the literature on consensus under switching topologies, *e.g.*, Arcak (2007). There are, however, noticeable differences. In the present case, the incidence matrix of the graph is a time-varying matrix satisfying: i) $\mathcal{B}(t) = 0$ in the presence of DoS; and ii) $\mathcal{B}(t) = \mathcal{B}$ in the absence of DoS, where $\mathcal{B}$ represents the incidence matrix related to the nominal graph configuration. Consider now a DoS pattern consisting of countable number of singletons, namely $\Xi(0, t) = \bigcup_{n \in \mathbb{Z}_{\geq 0}} \{h_n\}$, with $\Lambda_n \leq \Delta_*$. It is trivial to conclude that there exist constant $\delta \in \mathbb{R}_{>0}$ and $\alpha \in \mathbb{R}_{>0}$ such that (*cf.* Arcak (2007))

$$\int_{t_0}^{t_0+\delta} Q\mathcal{B}(t)\mathcal{B}^\top(t)Q^\top dt = Q\mathcal{B}\mathcal{B}^\top Q^\top \delta > \alpha I$$

for all $t_0 \in \mathbb{R}_{\geq 0}$, where Q is a suitable projection matrix. However, in accordance with the previous discussion, consensus can be destroyed. The subtle, yet important, difference is due to the constraint on the frequency of the information exchange that is imposed by the network. In this sense, the notion of PoC naturally extends the PoE condition to digital networked settings by requiring that the graph connectivity be established over periods of time that are consistent with the constraints imposed by the communication medium.

2.2.2 CONVERGENCE ANALYSIS

This section is devoted to the proof of Proposition 2.1 and 2.2 and Theorem 2.2.

Proof of Proposition 2.1. Let

$$V(x(t)) = \frac{1}{2}x^T(t)Lx(t)$$

where $t \geq 0$. Consider the evolution of $\dot{V}(t)$ along the solutions to (2.2). Following the same steps as in De Persis and Frasca (2013), it is easy to verify that

$$\dot{V}(x(t)) \leq - \sum_{i: |\operatorname{ave}_i(t_k^i)| \geq \varepsilon \ \wedge \ t_k^i \in \Theta(0,t)} \frac{\varepsilon}{2} \tag{2.19}$$

In words, the derivative of V decreases whenever, for some node i, two conditions are met: i) $|\operatorname{ave}_i(t_k^i)| \geq \varepsilon$, which means that node i has not reached the consensus set; and ii) communication is possible.

From (2.19) we deduce that there must exist a finite time T_1 such that, for every node i and every k with $t_k^i \geq T_1$, either $|\operatorname{ave}_i(t_k^i)| < \varepsilon$ or $t_k^i \in \Xi(0,t)$. This is because, otherwise, the function V would become negative contradicting the fact that V is non-negative definite since L is the Laplacian graph. Thus the proof follows simply by recalling that in both the cases $|\operatorname{ave}_i(t_k^i)| < \varepsilon$ and $t_k^i \in \Xi(0,t)$ the control u_i is set to zero.

Proof of Proposition 2.2 By definition of $\bar{\Xi}$ and in view of Assumption 2.1 and 2.2 , the following bounds on $\bar{\Xi}$ is readily obtained:

$$\begin{aligned} |\bar{\Xi}(\tau,t)| &\leq |\Xi(\tau,t)| + (n(\tau,t)+1)\Delta_* \\ &\leq \kappa + \frac{t-\tau}{\tau_d} + \left(\mu + \frac{t-\tau}{\tau_f} + 1\right)\Delta_* \end{aligned} \tag{2.20}$$

Finally notice that

$$|\bar{\Theta}(\tau,t)| = t - \tau - |\bar{\Xi}(\tau,t)| \tag{2.21}$$

Combining the two equations above, one sees that a sufficient condition for PoC is that $t - \tau > |\bar{\Xi}(\tau,t)|$, which, in turn, is implied by

$$t - \tau > \kappa + \frac{t-\tau}{\tau_d} + \left(\mu + \frac{t-\tau}{\tau_f} + 1\right)\Delta_* \tag{2.22}$$

This is equivalent to

$$\left(1 - \varphi(\tau_f, \tau_d, \Delta_*)\right)(t-\tau) > \kappa + (1+\mu)\Delta_* \tag{2.23}$$

which concludes the proof.

Proof of Theorem 2.2. The proof follows immediately by combining Proposition 2.1 and 2.2. In fact, by Proposition 2.1, all the local controls converge to zero in a finite time. In turn, Proposition 2.2 excludes the possibility that this is due to a persistence of the DoS status. This means that convergence to the set $\mathcal{E}$ is necessarily achieved.

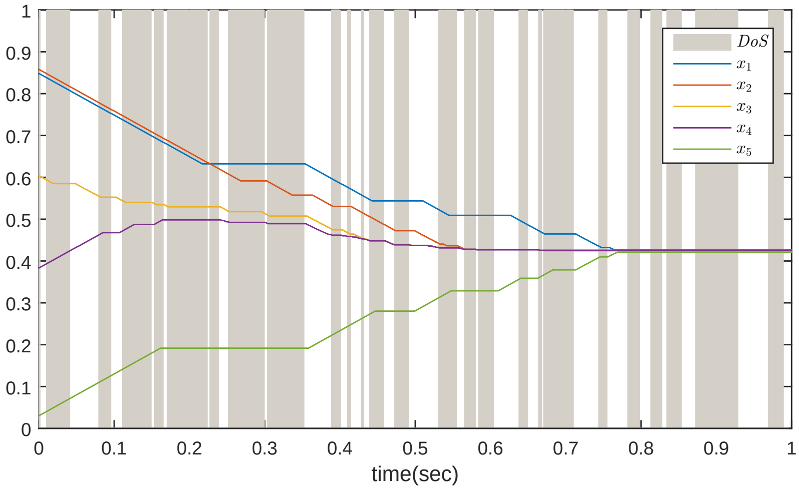

Figure 2.1: Evolution of state x, corresponding to the solution of (2.2) and (2.12), with $\varepsilon = 0.02$ (a complete graph with $n = 5$ nodes) in presence of DoS with an average duty cycle of $\sim 55\%$. The vertical grey stripes represent the time-intervals over which DoS is active.

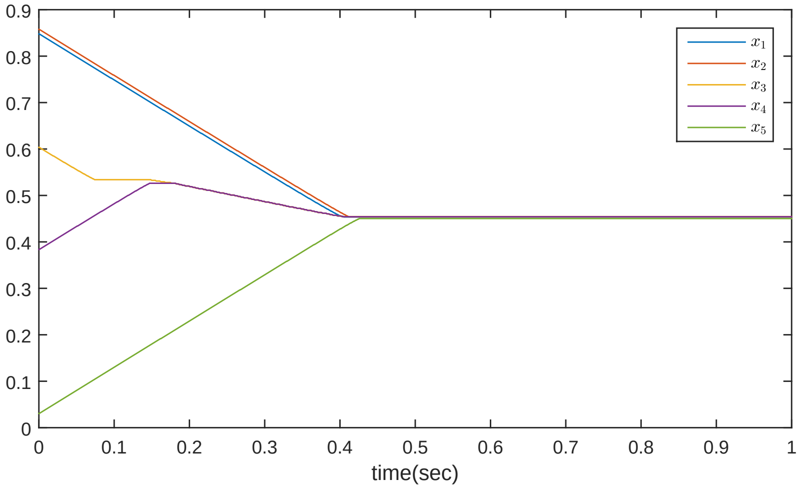

Figure 2.2: Evolution of state x, corresponding to the solution of (2.2) and (2.12), with $\varepsilon = 0.02$ (a complete graph with $n = 5$ nodes) in absence of DoS.

2.3 A NUMERICAL EXAMPLE

In what follows we see a numerical example of the proposed consensus protocol in presence of DoS. A sustained DoS attack with variable period and duty cycle, generated randomly. The resulting DoS signal has an average duty cycle of 55%.

We assume completely connected undirected graph with $n = 5$ nodes. During times over which communication is possible each agent is connected to the other agents, namely $d^i = 4$, while in presence of DoS graph becomes edgeless. A sample evolution of (2.2) and (2.12) with $\varepsilon = 0.02$ starting from the same initial condition and on the same graph is depicted in Figure 2.1 and Figure 2.2. Initial conditions are generated randomly between 0 and 1. The vertical gray stripes in Figure 2.1 represent the time-intervals over which DoS is active. The values of τ_d and τ_f for which consensus is not destroyed are plotted in Figure 2.3. Values above this curve satisfy inequality (2.17) with $\Delta_* = 0.0013$.

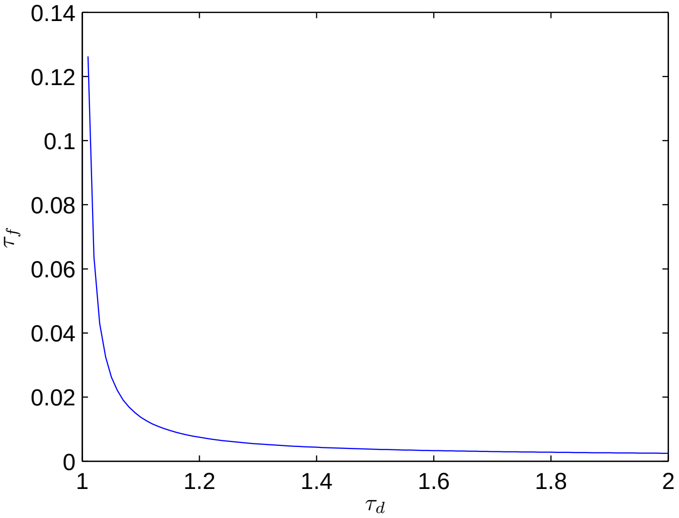

Figure 2.3: Locus of the points where $1/\tau_d + \Delta_*/\tau_f = 1$ with $\Delta_* = 0.0013$. The values above the curve satisfies condition (2.17).

Consistent with the results in De Persis and Frasca (2013); Cortés (2006), the solution to (2.2) and (2.12) in the absence of DOS converges in finite time to a value close to average-max min-consensus, namely $\frac{1}{2}(\min_i x_i(0) + \max_i x_i(0))$. Furthermore, one sees that the presence of DoS slows down convergence. This is due to controls remaining constantly to zero during the DoS status. The consensus time in Figure 2.1 is almost twice the consensus time in Figure 2.2.

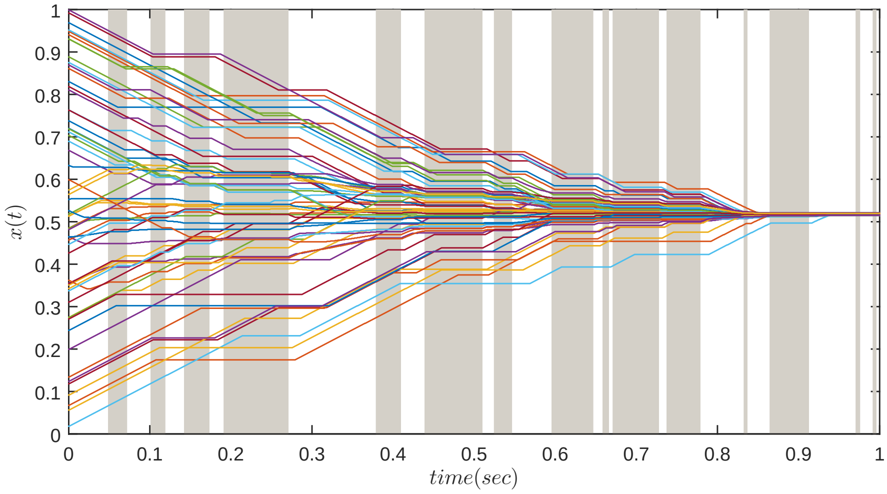

Figure 2.4: Evolution of state x in presence of DoS, average duty cycle $\sim 48\%$

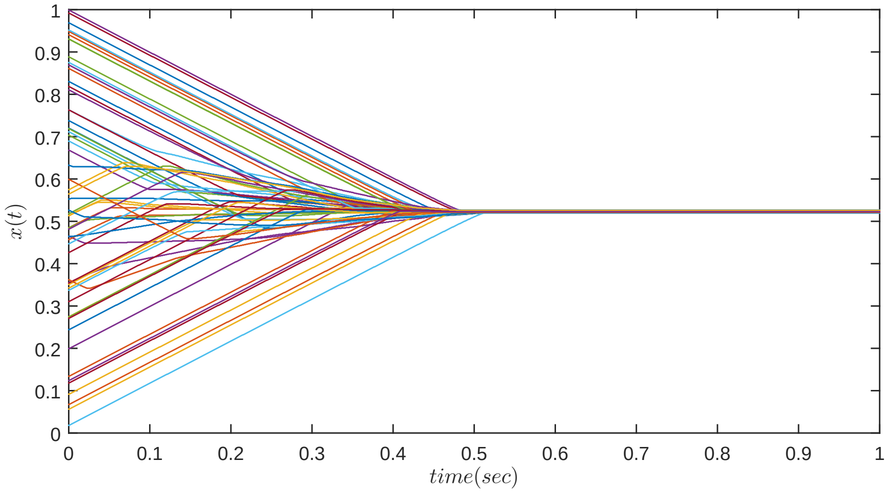

Figure 2.5: Evolution of state x in the absence of DoS.

To further observe the performance of the proposed resilient coordination protocol, we consider a large connected and undirected network comprised of

$n = 60$ nodes where each nodes is randomly connected to 10 neighbors, i.e. $d^i = 10$. The coordination parameters are as before, but a new random DoS is considered with an average duty cycle of $\sim 48\%$. The simulation results for the new example are given in Figure 2.4 and Figure 2.5.

3

Jamming-resilient Coordination over Peer-to-Peer Networks

ABSTRACT

In this chapter, in a slightly different approach than chapter 2, a general framework is considered in which the network links can fail independent of each other. By introducing the notion of Persistency-of-Communication (PoC), we provide an explicit characterization of DoS frequency and duration under which consensus can be preserved by suitably designing time-varying control and communication policies. An explicit characterization of the effects of DoS on the consensus time is also provided. The considered notion of PoC is compared with classic average connectivity conditions that are found in pure continuous-time consensus networks. Finally, examples are given to substantiate the analysis.

Published as:

D. Senejohnny, P. Tesi, and C. De Persis, "A jamming-resilient algorithm for self-triggered network coordination," *IEEE Transactions on Control of Network Systems, In Press*, 2017.

3.1 THE FRAMEWORK: SELF-TRIGGERED CONSENSUS

Motivated by a change in communication network form “infrastructure” mode to “ad-hoc” (peer-to-peer), the self-triggered consensus framework adopted in this chapter is rather different than the framework in chapter 2. This is further elaborated in 3.1.3.

3.1.1 SYSTEM DEFINITION

We consider a consensus network, which is represented by an undirected graph $\mathcal{G} = (\mathcal{I}, \mathcal{E})$, where $\mathcal{I} = \{1, \ldots, n\}$ denotes the node set and $\mathcal{E} \subseteq \mathcal{I} \times \mathcal{I}$ denotes the edge set. Specifically, we denote by D and L the incidence and Laplacian matrix of $\mathcal{G}$, respectively. For each node $i \in \mathcal{I}$, we denote by $\mathcal{Q}_i$ the set of its neighbors, and by d^i the cardinality of $\mathcal{Q}_i$, that is $d^i = |\mathcal{Q}_i|$. Throughout the chapter, we shall refer to $\mathcal{G}$ as the “nominal” network, and we shall assume that $\mathcal{G}$ is connected.

The consensus network of interest employs *self-triggered* communication De Persis and Frasca (2013), defined via hybrid dynamics, with state variables $(x, u, \theta) \in \mathbb{R}^n \times \mathbb{R}^d \times \mathbb{R}^d$, where x is the vector of nodes states, u is the vector of controls, θ is the vector of clock variables, and d is the sum of the neighbors of all the nodes, *i.e.*, $d := \sum_{i=1}^{n} d^i$. The control signals are assumed to belong to $\mathcal{T} := \{-1, 0, +1\}$. The specific quantizer of choice is $\mathrm{sign}_\varepsilon : \mathbb{R} \to \mathcal{T}$, which is given by

$$\mathrm{sign}_\varepsilon(z) := \begin{cases} \mathrm{sign}(z) & \text{if } |z| \geq \varepsilon \\ 0 & \text{otherwise} \end{cases} \tag{3.1}$$

where $\varepsilon > 0$ is a sensitivity parameter, which can be used at the design stage for trading-off frequency of the transmissions vs. accuracy of the consensus region.

The system $(x, u, \theta) \in \mathbb{R}^n \times \mathbb{R}^d \times \mathbb{R}^d$ satisfies the continuous evolution

$$\begin{cases} \dot{x}^i = \sum_{j \in \mathcal{Q}_i} u^{ij} \\ \dot{u}^{ij} = 0 \\ \dot{\theta}^{ij} = -1 \end{cases} \tag{3.2}$$

where $i \in \mathcal{I}$ and $j \in \mathcal{Q}_i$. The system satisfies the differential equation above for all t except for those values of the time at which the set

$$\mathcal{J}(\theta, t) = \{(i,j) \in \mathcal{I} \times \mathcal{I} \ : \ j \in \mathcal{Q}_i \text{ and } \theta^{ij}(t^-) = 0\} \tag{3.3}$$

is non-empty, where $s(t^-)$ denotes the limit from below of a signal $s(t)$, *i.e.*, $s(t^-) = \lim_{\tau \nearrow t} s(\tau)$. At these time instants, in the "nominal" operating mode (when communication is allowed), a discrete transition occurs, which is governed by the following discrete update:

$$\begin{cases} x^i(t) = x^i(t^-) \quad \forall i \in \mathcal{I} \\ u^{ij}(t) = \begin{cases} \operatorname{sign}_\varepsilon\big(\mathcal{D}^{ij}(t)\big) & \text{if } (i,j) \in \mathcal{J}(\theta, t) \\ u^{ij}(t^-) & \text{otherwise} \end{cases} \\ \theta^{ij}(t) = \begin{cases} f^{ij}(x(t)) & \text{if } (i,j) \in \mathcal{J}(\theta, t) \\ \theta^{ij}(t^-) & \text{otherwise} \end{cases} \end{cases} \tag{3.4}$$

where for every $i \in \mathcal{I}$ and $j \in \mathcal{Q}_i$, the map $f^{ij} : \mathbb{R}^n \to \mathbb{R}_{>0}$ is defined as

$$f^{ij}(x(t)) := \begin{cases} \dfrac{|\mathcal{D}^{ij}(t)|}{2(d^i + d^j)} & \text{if } |\mathcal{D}^{ij}(t)| \geq \varepsilon \\ \dfrac{\varepsilon}{2(d^i + d^j)} & \text{if } |\mathcal{D}^{ij}(t)| < \varepsilon \end{cases} \tag{3.5}$$

and

$$\mathcal{D}^{ij}(t) = x^j(t) - x^i(t) \tag{3.6}$$

The functioning of (3.2)-(3.6) can be described as follows. Each linked pair of nodes is equipped with a local clock. When the clock θ^{ij} reaches 0, neighboring nodes i and j exchange information and θ^{ij} is reset to a value that depends on $\mathcal{D}^{ij}$, that is the relative difference between x^i and x^j. At the same time, nodes i and j also update their controls based on $\mathcal{D}^{ij}$. The control action is fully distributed since the evolution of a node x^i only depends on x^j with $j \in \mathcal{N}_i$. The term "self-triggered", first used in the context of real-time systems Velasco et al. (2003), stems from the fact that the next update time (the value of θ^{ij}) is precomputed at the update time, in contrast with "event-triggered" policies in which the updates are activated based on the continuous monitoring of a triggering condition Heemels et al. (2012).

3.1.2 MODIFICATION OF THE COORDINATION PROTOCOL:

In chapter 2, due to an "infrastructure" mode communication network, all the links can fail simultaneously under DoS. In an "ad-hoc" (peer-to-peer) communication network, however, the situation is different. In such networks, communication links can fail independently and asynchronously. Therefore, to capture the effect of DoS over a peer-to-peer network some modifications are necessary in the coordination protocol (2.2)-(2.4). In the coordination protocol in 3.1.1, a clock and controller is associated to each edge $(i, j) \in \mathcal{E}$, as in De Persis and Frasca (2013). The overall control law given in (3.2) is summation of edge controllers. In the modified framework edge controllers (3.4) and clocks (3.5) can be appropriately designed to acheive resiliency against DoS. This is further elaborated in section 3.3.1 .

3.1.3 PROTOTYPICAL RESULT FOR SELF-TRIGGERED CONSENSUS

The following result characterizes the limiting behavior of the system (3.2)-(3.4).

Theorem 3.1. *De Persis and Frasca (2013) Let x be the solution to (3.2)-(3.4). Then, for every initial condition, x converges in finite time to a point $x^* \in \mathbb{R}^n$ belonging to the set*

$$\mathcal{E} = \{x \in \mathbb{R}^n \ : \ |x^i(t) - x^j(t)| < \delta \quad \forall\, (i,j) \in \mathcal{I} \times \mathcal{I}\} \tag{3.7}$$

where $\delta = \varepsilon(n-1)$.

Theorem 3.1 will be used as a reference frame for the analysis of Section 3.3 and 3.4. This theorem is prototypical in the sense that it serves to illustrate the salient features of the problem of consensus/coordination in the presence of communication interruptions. Following De Persis and Frasca (2013), the analysis of this chapter could be extended to include important aspects such as *quantized communication*, *delays* and *asymptotic consensus* (rather than approximate consensus as in (3.7)). While important, these aspects do not add much to the present investigation and will be therefore omitted. We refer the interested reader to De Persis and Frasca (2013) for a discussion on how these aspects can be dealt with.

3.2 PROBLEM FORMULATION: NETWORK RESILIENCE AGAINST DOS

We shall refer to Denial-of-Service (DoS, in short) as the phenomenon by which communication between the network nodes is interrupted. We shall consider the very general scenario in which the network communication links can fail independent of each other. From the perspective of modeling, this amounts to considering multiple DoS signals, one for each network communication link.

3.2.1 ASSUMPTIONS: CLASS OF DOS SIGNALS

Let $\{h_n^{ij}\}_{n\in\mathbb{Z}_{\geq 0}}$ with $h_0^{ij}\geq 0$ denote the sequence of DoS off/on transitions affecting the link $\{i,j\}$, namely the sequence of time instants at which the DoS status on the link $\{i,j\}$ exhibits a transition from zero (communication is possible) to one (communication is interrupted). Then

$$H_n^{ij} := \{h_n^{ij}\} \cup \Big[h_n^{ij}, h_n^{ij} + \tau_n^{ij}\Big[\tag{3.8}$$

represents the n-th DoS time-interval, of a length $\tau_n^{ij} \in \mathbb{R}_{\geq 0}$, during which communication on the link $\{i,j\}$ is not possible. Given t, $\tau \in \mathbb{R}_{\geq 0}$, with $t \geq \tau$, let

$$\Xi^{ij}(\tau,t) := \bigcup_{n\in\mathbb{Z}_{\geq 0}} H_n^{ij} \bigcap [\tau,t] \tag{3.9}$$

and

$$\Theta^{ij}(\tau,t) := [\tau,t] \setminus \Xi^{ij}(\tau,t) \tag{3.10}$$

where $\setminus$ denotes relative complement. In words, for each interval $[\tau,t]$, $\Xi^{ij}(\tau,t)$ and $\Theta^{ij}(\tau,t)$ represent the sets of time instants where communication on the link $\{i,j\}$ is denied and allowed, respectively.

The first question to be addressed is that of determining a suitable modeling framework for DoS. Following De Persis and Tesi (2015), we consider a general model that only constrains DoS attacks in terms of their average frequency and duration. Let $n^{ij}(\tau,t)$ denote the number of DoS off/on transitions on the link $\{i,j\}$ occurring on the interval $[\tau,t]$.

Assumption 3.1 (DoS frequency). *For each $\{i,j\} \in \mathcal{E}$, there exist $\mu^{ij} \in \mathbb{R}_{\geq 0}$ and $\tau_f^{ij} \in \mathbb{R}_{>0}$ such that*

$$n^{ij}(\tau,t) \leq \mu^{ij} + \frac{t-\tau}{\tau_f^{ij}} \tag{3.11}$$

for all $t, \tau \in \mathbb{R}_{\geq 0}$ with $t \geq \tau$.

Assumption 3.2 (DoS duration). *For each $\{i,j\} \in \mathcal{E}$, there exist $\kappa^{ij} \in \mathbb{R}_{\geq 0}$ and $\tau_d^{ij} \in \mathbb{R}_{>1}$ such that*

$$|\Xi^{ij}(\tau,t)| \leq \kappa^{ij} + \frac{t-\tau}{\tau_d^{ij}} \tag{3.12}$$

for all $t, \tau \in \mathbb{R}_{\geq 0}$ with $t \geq \tau$.

In Assumption 3.1, the term "frequency" stems from the fact that τ_f^{ij} provides a measure of the "dwell-time" between any two consecutive DoS intervals on the link $\{i,j\}$. The quantity μ^{ij} is needed to render (3.11) self-consistent when $t = \tau = h_n^{ij}$ for some $n \in \mathbb{Z}_{\geq 0}$, in which case $n^{ij}(\tau,t) = 1$. Likewise, in Assumption 3.2, the term "duration" is motivated by the fact that τ_d^{ij} provides a measure of the fraction of time ($\tau_d^{ij} > 1$) the link $\{i,j\}$ is under DoS. Like μ^{ij}, the constant κ^{ij} plays the role of a regularization term. It is needed because during a DoS interval, one has $|\Xi^{ij}(h_n^{ij}, h_n^{ij} + \tau_n^{ij})| = \tau_n^{ij} \geq \tau_n^{ij}/\tau_d^{ij}$ since $\tau_d^{ij} > 1$, with $\tau_n^{ij} = \tau_n^{ij}/\tau_d^{ij}$ if and only if $\tau_n^{ij} = 0$. Hence, κ^{ij} serves to make (3.12) self-consistent. Thanks to the quantities μ^{ij} and κ^{ij}, DoS frequency and duration are both average quantities. Figure 3.1 exemplifies values of $n^{ij}(\tau,t)$ and $\Xi^{ij}(\tau,t)$ for a given DoS pattern on the link $\{i,j\}$.

Remark 3.1. Throughout this chapter, we will mostly focus on the case where DoS is caused by malicious attacks. Of course, DoS might also result from a "genuine" network congestion. We shall address this case in Section 3.4.3.

3.2.2 CONTROL OBJECTIVE

The control objective is to design variants to the basic protocol (3.4)-(3.6) that guarantee robustness against the class of DoS signals described in Section 3.2.1, *i.e.*, variants that preserve consensus despite the occurrence of periods of DoS.

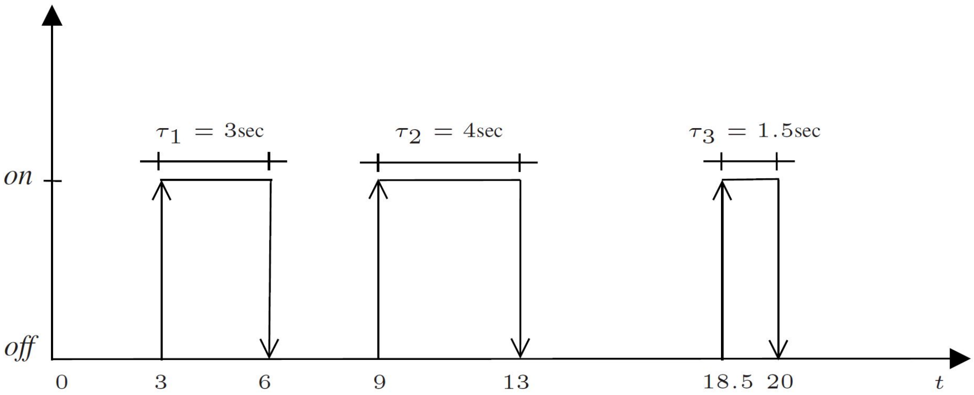

Figure 3.1: Example of DoS signal on the link $\{i, j\}$. *Off/on* transitions are represented as ↑, while *on/off* transitions are represented as ↓. The *off/on* transitions occur at 3sec, 9sec and 18.5sec, and the corresponding intervals have duration 3sec, 4sec and 1.5sec, respectively. This yields for instance: $n^{ij}(0,1) = 0$, $n^{ij}(1,10) = 2$ and $n^{ij}(10,20) = 1$, while $\Xi^{ij}(0,1) = \emptyset$, $\Xi^{ij}(1,10) = [3,6[\cup [9,10[$ and $\Xi^{ij}(10,20) = [10,13[\cup [18.5,20[$.

We will show in Section 3.3 that variants do exist that rely on a modification of both control and communication protocols. In this respect, we will provide an explicit characterization of DoS frequency and duration $(\tau_f^{ij}, \tau_d^{ij})$ at the various network links under which consensus can be preserved. We will also provide an explicit characterization of the effects of DoS on the consensus time.

3.3 DOS-RESILIENT CONSENSUS

3.3.1 MODIFIED CONSENSUS PROTOCOL

In order to achieve robustness against DoS, the nominal discrete evolution (3.4) is modified as follows:

$$\begin{cases} x^i(t) = x^i(t^-) \quad \forall i \in \mathcal{I} \\ u^{ij}(t) = \begin{cases} \operatorname{sign}_\varepsilon\big(\mathcal{D}^{ij}(t)\big) & \text{if } (i,j) \in \mathcal{J}(\theta,t) \wedge t \in \Theta^{ij}(0,t) \\ 0 & \text{if } (i,j) \in \mathcal{J}(\theta,t) \wedge t \in \Xi^{ij}(0,t) \\ u^{ij}(t^-) & \text{otherwise} \end{cases} \\ \theta^{ij}(t) = \begin{cases} f^{ij}(x(t)) & \text{if } (i,j) \in \mathcal{J}(\theta,t) \wedge t \in \Theta^{ij}(0,t) \\ \dfrac{\varepsilon}{2(d^i+d^j)} & \text{if } (i,j) \in \mathcal{J}(\theta,t) \wedge t \in \Xi^{ij}(0,t) \\ \theta^{ij}(t^-) & \text{otherwise} \end{cases} \end{cases} \tag{3.13}$$

In words, the control action u^{ij} is reset to zero whenever the link $\{i,j\}$ is in DoS status. Notice that this requires that the nodes are able to detect the occurrence of DoS. This is the case, for instance, with transmitters employing carrier sensing as medium access policy. Under such circumstances, a DoS signal in the form of *constant jamming* (*cf.* Section 3.2.2) can be detected. Another example is when transceivers use Transmission Control Protocol (TCP) acknowledgment and DoS takes the form of *reactive jamming* (*cf.* Section 3.2.2). In addition to u, also the local clocks are modified upon DoS, yielding a *two-mode* sampling logic. In particular, for each $\{i,j\} \in \mathcal{E}$, let $\{t_k^{ij}\}_{k\in\mathbb{Z}_{\geq 0}}$ denote the sequence of transmission attempts. Then, each θ^{ij} satisfies

$$t_{k+1}^{ij} = t_k^{ij} + \begin{cases} f^{ij}(x(t_k^{ij})) & \text{if } t_k^{ij} \in \Theta^{ij}(0,t) \\ \dfrac{\varepsilon}{2(d^i+d^j)} & \text{otherwise} \end{cases} \tag{3.14}$$

As it will become clear later on, this is in order to maximize the robustness of the consensus protocol against DoS. By (3.14), it is an easy matter to see that for each $\{i,j\} \in \mathcal{E}$ the sequences $\{t_k^{ij}\}_{k\in\mathbb{Z}_{\geq 0}}$ satisfy a "dwell-time" property, since

$$\Delta_k^{ij} := t_{k+1}^{ij} - t_k^{ij} \geq \frac{\varepsilon}{4d_{\max}} \tag{3.15}$$

for all $k \in \mathbb{R}_{\geq 0}$, where $d_{max} = \max_{i\in\mathcal{I}} d^i$. This ensures that all the sequences of transmission times are Zeno-free.

Similar to (3.4)-(3.6), also the modified consensus protocol does only require local clocks. In addition, the control action remains fully distributed since the evolution of a node x^i only depends on x^j with $j \in \mathcal{N}_i$.

For the sake of clarity, the DoS-resilient consensus protocol is summarized below.

DoS-resilient consensus protocol

```
initialization: For all $i \in \mathcal{I}$ and $j \in \mathcal{N}_i$, set $\theta^{ij}(0^-) = 0$, $u^{ij}(0^-) \in \{-1, 0, +1\}$,
and $u^i(0^-) = \sum_{j \in \mathcal{N}_i} u^{ij}(0^-)$;
for all $i \in \mathcal{I}$ do
    for all $j \in \mathcal{N}_i$ do
        while $\theta^{ij}(t) > 0$ do
            $i$ applies the control $u^i(t) = \sum_{j \in \mathcal{N}_i} u^{ij}(t)$;
        end while
        if $\theta^{ij}(t^-) = 0 \wedge t \in \Theta^{ij}(0, t)$ then
            $i$ updates $u^{ij}(t) = \mathrm{sign}_\varepsilon\big(x^j(t) - x^i(t)\big)$;
            $i$ updates $\theta^{ij}(t) = f^{ij}(x(t))$;
        else
            if $\theta^{ij}(t^-) = 0 \wedge t \in \Xi^{ij}(0, t)$ then
                $i$ updates $u^{ij}(t) = 0$;
                $i$ updates $\theta^{ij}(t) = \dfrac{\varepsilon}{2(d^i + d^j)}$;
            end if
        end if
    end for
end for
```

3.3.2 CONVERGENCE OF THE SOLUTIONS AND δ-CONSENSUS

We are now in position to characterize the overall network behavior in the presence of DoS. In this respect, the analysis is subdivided into two main steps: i) we first prove that all the network nodes eventually stop to update their local controls; and ii) we then provide conditions on the DoS frequency and duration such that consensus, in the sense of (3.7), is preserved. The latter property is achieved by resorting to a notion of *Persistency-of-Communication*, which determines the amount of DoS (frequency and duration) under which consensus can be preserved.

As for i), the following result holds true.

Proposition 3.1. (Convergence of the solutions) *Let x be the solution to* (3.2) *and* (3.13)*. Then, for every initial condition, there exists a finite time T_* such that, for any $i \in \mathcal{I}$, it holds that $u^i(t) = 0$ for all $t \geq T_*$.*

Proof. Consider the Lyapunov function

$$V(x) = \frac{1}{2} x^\top x \tag{3.16}$$

Let $t_k^{ij} := \max\{t_\ell^{ij} : t_\ell^{ij} \leq t, \ell \in \mathbb{Z}_{\geq 0}\}$. First notice that the derivative of V along the solutions to (3.2) satisfies

$$\begin{aligned}
\dot{V}(x(t)) &= \sum_{i=1}^{n} x^i(t)\dot{x}^i(t) \\
&= \sum_{i=1}^{n} [x^i(t) \sum_{j \in \mathcal{N}_i} u^{ij}(t)] \\
&= - \sum_{\substack{\{i,j\} \in \mathcal{E}: \\ |\mathcal{D}^{ij}(t_k^{ij})| \geq \varepsilon \,\wedge\, t_k^{ij} \in \Theta^{ij}(0,t)}} \mathcal{D}^{ij}(t) \operatorname{sign}_\varepsilon(\mathcal{D}^{ij}(t_k^{ij})) \\
&\leq - \sum_{\substack{\{i,j\} \in \mathcal{E}: \\ |\mathcal{D}^{ij}(t_k^{ij})| \geq \varepsilon \,\wedge\, t_k^{ij} \in \Theta^{ij}(0,t)}} \frac{|\mathcal{D}^{ij}(t_k^{ij})|}{2}
\end{aligned} \tag{3.17}$$

In words, the derivative of V decreases whenever, for some $\{i,j\} \in \mathcal{E}$, two conditions are met: i) $|\mathcal{D}^{ij}(t_k^{ij})| \geq \varepsilon$, which means that i and j are not ε-close; and ii) communication on the link that connects i and j is possible. The third equality follows from the fact that for any $\{i,j\} \in \mathcal{E}$ for which $|\mathcal{D}^{ij}(t_k^{ij})| < \varepsilon$ or $t_k^{ij} \in \Xi^{ij}(0,t)$ we have $u^{ij}(t) = 0$ for all $[t_k^{ij}, t_{k+1}^{ij}[$, and the fact that $u^{ij}(t) = \operatorname{sign}_\varepsilon(\mathcal{D}^{ij}(t_k^{ij}))$ where $\mathcal{D}^{ij}(t) = x^j(t) - x^i(t)$. The inequality follows from the fact that, during the continuous evolution $|\dot{\mathcal{D}}^{ij}(t)| \leq d^i + d^j$ and at the jumps $\mathcal{D}^{ij}(t)$ does not change its value. This implies that $\mathcal{D}^{ij}(t)$ cannot differ from $\mathcal{D}^{ij}(t_k^{ij})$ in absolute value for more than $(d^i + d^j)(t - t_k^{ij})$. Exploiting this fact, if communication is allowed and $|\mathcal{D}^{ij}(t_k^{ij})| \geq \varepsilon$ then by (3.5) and (3.14) we have

$$|\mathcal{D}^{ij}(t)| \geq |\mathcal{D}^{ij}(t_k^{ij})|/2 \tag{3.18}$$

and

$$\operatorname{sign}_\varepsilon(\mathcal{D}^{ij}(t)) = \operatorname{sign}_\varepsilon(\mathcal{D}^{ij}(t_k^{ij})) \tag{3.19}$$

for all $t \in [t_k^{ij}, t_{k+1}^{ij}[$.

From (3.17) there must exist a finite time T_* such that, for every $\{i,j\} \in \mathcal{E}$ and every k with $t_k^{ij} \geq T_*$, it holds that $|\mathcal{D}^{ij}(t_k^{ij})| < \varepsilon$ or $t_k^{ij} \in \Xi^{ij}(0,t)$. This is because, otherwise, V would become negative. The proof follows recalling that in both the cases $|\mathcal{D}^{ij}(t_k^{ij})| < \varepsilon$ and $t_k^{ij} \in \Xi^{ij}(0,t)$ the control $u^{ij}(t)$ is set equal to zero.

The above result does not allow one to conclude anything about the final disagreement vector in the sense that given a pair of nodes (i,j) the asymptotic value of $|x^j(t) - x^i(t)|$ can be arbitrarily large. As an example, if node i is never allowed to communicate then $x^i(t) = x^i(0)$ for all $t \in \mathbb{R}_{\geq 0}$. In order to recover the same conclusions as in Theorem 3.1, bounds on DoS frequency and duration have to be enforced. The result which follows provides one such characterization.

Let $\{i,j\} \in \mathcal{E}$ be a generic network link, and consider a DoS sequence on $\{i,j\}$, which satisfies Assumption 3.1 and 3.2. Define

$$\alpha^{ij} := \frac{1}{\tau_d^{ij}} + \frac{\Delta_*^{ij}}{\tau_f^{ij}} \tag{3.20}$$

where

$$\Delta_*^{ij} := \frac{\varepsilon}{2(d^i + d^j)} \tag{3.21}$$

Proposition 3.2 (Link Persistency-of-Communication (PoC)). *Consider any link $\{i,j\} \in \mathcal{E}$ employing the transmission protocol* (3.13)*. Also consider any DoS sequence on $\{i,j\}$, which satisfies Assumption 3.1 and 3.2 with μ^{ij} and κ^{ij} arbitrary, and τ_d^{ij} and τ_f^{ij} such that $\alpha^{ij} < 1$. Let*

$$\Phi^{ij} := \frac{\kappa^{ij} + (\mu^{ij} + 1)\Delta_*^{ij}}{1 - \alpha^{ij}} \tag{3.22}$$

Then, for any given unsuccessful transmission attempt t_k^{ij}, at least one successful transmission occurs over the link $\{i,j\}$ within the interval $[t_k^{ij}, t_k^{ij} + \Phi^{ij}]$.

Proof. Consider any link $\{i,j\} \in \mathcal{E}$, and suppose that a certain transmission attempt t_k^{ij} is unsuccessful. We claim that a successful transmission over $\{i,j\}$ does always occur within $[t_k^{ij}, t_k^{ij} + \Phi^{ij}]$. We prove the claim by contradiction. To this end, we first introduce some auxiliary quantities. Let $\bar{H}_n^{ij} := \{h_n^{ij}\} \cup [h_n^{ij}, h_n^{ij} + \tau_n^{ij} + \Delta_*^{ij}[$. denote the n-th DoS interval over the link $\{i,j\}$ prolonged by Δ_*^{ij} units of time. Also let

$$\begin{aligned} \bar{\Xi}^{ij}(\tau,t) &:= \bigcup_{n \in \mathbb{Z}_{\geq 0}} \bar{H}_n^{ij} \bigcap [\tau, t] \\ \bar{\Theta}^{ij}(\tau,t) &:= [\tau,t] \setminus \bar{\Xi}^{ij}(\tau,t) \end{aligned} \tag{3.23}$$

Suppose then that the claim is false, and let t_* denote the last transmission attempt over $[t_k^{ij}, t_k^{ij} + \Phi^{ij}]$. Notice that this necessarily implies $|\bar{\Theta}^{ij}(t_k^{ij}, t_*)| = 0$. To see this, first note that, in accordance with (3.14), the inter-sampling time over the interval $[t_k^{ij}, t_*]$ is equal to $\varepsilon/(2(d^i + d^j)) = \Delta_*^{ij}$. Hence, we cannot have $|\bar{\Theta}^{ij}(t_k^{ij}, t_*)| > 0$ since this would imply the existence of a DoS-free interval within $[t_k^{ij}, t_*]$ of length greater than Δ_*^{ij}, which is not possible since, by hypothesis, no successful transmission attempt occurs within $[t_k^{ij}, t_*]$. Thus $|\bar{\Theta}^{ij}(t_k^{ij}, t_*)| = 0$. Moreover, since t_* is unsuccessful, it must be contained in a DoS interval, say H_q^{ij}. This implies $[t_*, t_* + \Delta_*^{ij}[\subseteq \bar{H}_q^{ij}$ Hence,

$$\begin{aligned} |\bar{\Theta}(t_k^{ij}, t_* + \Delta_*^{ij})| &= |\bar{\Theta}(t_k^{ij}, t_*)| + |\bar{\Theta}(t_*, t_* + \Delta_*^{ij})| \\ &= 0 \end{aligned}$$

However, condition $|\bar{\Theta}(t_k^{ij}, t_* + \Delta_*^{ij})| = 0$ is not possible. To see this, simply notice that

$$\begin{aligned} |\bar{\Theta}(t_k^{ij}, t)| &= t - t_k^{ij} - |\bar{\Xi}(t_k^{ij}, t)| \\ &\geq t - t_k^{ij} - |\Xi(t_k^{ij}, t)| - (n(t_k^{ij}, t) + 1)\Delta_*^{ij} \\ &\geq (t - t_k^{ij})(1 - \alpha^{ij}) - \kappa^{ij} - (\mu^{ij} + 1)\Delta_*^{ij} \end{aligned} \tag{3.24}$$

for all $t \geq t_k^{ij}$ where the first inequality follows from the definition of the set $\bar{\Xi}(\tau, t)$ while the second one follows from Assumption 3.1 and 3.2. Hence, by (3.24), we have $|\bar{\Theta}(t_k^{ij}, t)| > 0$ for all $t > t_k^{ij} + (1-\alpha^{ij})^{-1}(\kappa^{ij} + (\mu^{ij}+1)\Delta_*^{ij}) = t_k^{ij} + \Phi^{ij}$. Accordingly, $|\bar{\Theta}(t_k^{ij}, t_* + \Delta_*^{ij})| = 0$ cannot occur because $t_* + \Delta_*^{ij} > t_k^{ij} + \Phi^{ij}$. In fact, by hypothesis, t_* is defined as the last unsuccessful transmission attempt within $[t_k^{ij}, t_k^{ij} + \Phi^{ij}]$, and, by (3.14), the next transmission attempt after t_* occurs at time $t_* + \Delta_*^{ij}$. This concludes the proof.

We refer to the property above as a PoC condition since this property guarantees that DoS does not permanently destroy communication. Combining Proposition 3.1 and 3.2, the main result of this section can be stated.

Theorem 3.2. *Let x be the solution to* (3.2) *and* (3.13)*. For each $\{i,j\} \in \mathcal{E}$, consider any DoS sequence that satisfies Assumption 3.1 and 3.2 with μ^{ij} and κ^{ij} arbitrary, and τ_d^{ij} and τ_f^{ij} such that $\alpha^{ij} < 1$. Then, for every initial condition, x converges in finite time to a point x^* belonging to the set $\mathcal{E}$ as in (3.7).*

Proof. By Proposition 3.1, all the local controls become zero in a finite time T_*. In turns, Proposition 3.2 excludes that this is due to the persistence of a DoS status. This means that, for all $\{i,j\} \in \mathcal{E}$, $|\mathcal{D}^{ij}(t)| = |x^j(t) - x^i(t)| < \varepsilon$ for all $t \geq T_*$. Since each pair of neighboring nodes differs by at most ε and the nominal graph is connected, we conclude that each pair of network nodes can differ by at most $\delta = \varepsilon(n-1)$.

3.3.3 CONVERGENCE TIME

The above theorem shows that convergence is reached in a finite time. The following result characterizes the effect of DoS on the convergence time.

Lemma 3.1 (Bound on the convergence time)**.** *Consider the same assumptions as in Theorem 3.1. Then,*

$$T_* \leq \left[\frac{1}{\varepsilon} + \frac{d_{\max}}{\varepsilon d_{\min}} + \frac{4d_{\max}}{\varepsilon^2}\Phi\right] \sum_{i\in\mathcal{I}} (x^i(0))^2 \tag{3.25}$$

where $d_{\min} := \min_{i\in\mathcal{I}} d^i$ and $\Phi := \max_{\{i,j\}\in\mathcal{E}} \Phi^{ij}$.

Proof. Consider the same Lyapunov function V as in the proof of Proposition 3.1. Notice that, by construction of the control law and the scheduling policy, for every successful transmission t_k^{ij} characterized by $|\mathcal{D}^{ij}(t_k^{ij})| \geq \varepsilon$, the function V decreases with rate not less than $\varepsilon/2$ for at least $\varepsilon/(4d_{\max})$ units of time. Hence, V decreases by a least $\varepsilon^2/(8d_{\max}) := \varepsilon_*$.Considering all the network links, such transmissions are in total no more than $\lfloor V(0)/\varepsilon_* \rfloor$ since, otherwise, the function V would become negative. Hence, it only remains to compute the time needed to have $\lfloor V(0)/\varepsilon_* \rfloor$ of such transmissions. In this respect, pick any $t_* \geq 0$ such that consensus has still not been reached. Note that we can have $u^{ij}(t_*) = 0$ for all $\{i,j\} \in \mathcal{E}$. However, this condition can last only for a limited amount of time. In fact, if $u^{ij}(t_*) = 0$ then the next transmission attempt, say ℓ^{ij}, over the link $\{i,j\}$ will necessarily occur at a time less than or equal to $t_* + \Delta_*^{ij}$ with $\Delta_*^{ij} \leq \varepsilon/(4d_{\min})$. Let $\mathcal{Q} := [t_*, t_* + \varepsilon/(4d_{\min})]$, and suppose that over $\mathcal{Q}$ all the controls u^{ij} have remained equal to zero. This implies that for some $\{i,j\} \in \mathcal{E}$ we necessarily have that ℓ^{ij} is unsuccessful. This is because if $u^{ij}(t) = 0$ for all $\{i,j\} \in \mathcal{E}$ and all $t \in \mathcal{Q}$ then $x^i(t) = x^i(t_*)$ for all $i \in \mathcal{I}$ and all $t \in \mathcal{Q}$. Hence, if all the ℓ^{ij} were successful, we should also have $u^{ij}(\ell^{ij}) \neq 0$ for some $\{i,j\} \in \mathcal{E}$ since, by hypothesis, consensus is not reached at time t_*. Hence, applying Proposition 3.2 we conclude that at least one of the controls u^{ij} will become non-zero before $\ell^{ij} + \Phi^{ij}$ units of time have elapsed. Overall, this implies that at least one control will become non-zero before $\varepsilon/(4d_{\min}) + \Phi$ units of time have elapsed. Since t_* is generic, we conclude that V decreases by at least ε_* every $\varepsilon/(4d_{\max}) + \varepsilon/(4d_{\min}) + \Phi$ units of time, which implies that

$$T_* \leq \left[\frac{\varepsilon}{4d_{\max}} + \frac{\varepsilon}{4d_{\min}} + \Phi \right] \frac{V(0)}{\varepsilon_*} \tag{3.26}$$

The thesis follows by recalling that $V(0)$ can be rewritten as $V(0) = \frac{1}{2} \sum_{i \in \mathcal{I}} (x^i(0))^2$.

3.4 DISCUSSION AND EXTENSIONS

3.4.1 PERSISTENCY-OF-COMMUNICATION AND CONSENSUS UNDER PERMANENT LINK DISCONNECTIONS

As it follows from the foregoing analysis, consensus is achieved whenever for each link $\{i,j\} \in \mathcal{E}$, the DoS signal satisfies $\alpha^{ij} < 1$. This condition poses limitations on both DoS frequency and duration. It is worth noting that this condition is in a wide sense also necessary in order to achieve consensus. To see this, consider a network for which removing the link $\{i,j\}$ causes the network underlying graph to be disconnected. Of course, if communication over $\{i,j\}$ is always denied then consensus cannot be achieved for arbitrary initial conditions. In this respect, it is an easy matter to see that condition $\alpha^{ij} < 1$ becomes necessary to achieve consensus. In fact, denote by $\mathcal{S}(\tau_f^{ij}, \tau_d^{ij})$ the class of all DoS signals for which $\alpha^{ij} \geq 1$. Then, $\mathcal{S}(\tau_f^{ij}, \tau_d^{ij})$ does always contain DoS signals for which communication over the link $\{i,j\}$ can be permanently denied. As an example, consider the DoS signal characterized by $(h_n^{ij}, \tau_n^{ij}) = (t_k^{ij}, 0)$. This DoS signal satisfies Assumption 3.1 and 3.2 with $(\mu^{ij}, \kappa^{ij}, \tau_f^{ij}, \tau_d^{ij}) = (1, 0, \Delta_*^{ij}, \infty)$, but destroys any communication attempt over the link $\{i,j\}$. As another example, consider the DoS signal characterized by $(h_0^{ij}, \tau_0^{ij}) = (0, \infty)$. This signal satisfies Assumption 3.1 and 3.2 with $(\mu^{ij}, \kappa^{ij}, \tau_f^{ij}, \tau_d^{ij}) = (1, 0, \infty, 1)$, but, as before, destroys any communication attempt over the link $\{i,j\}$. In both the examples, $\alpha^{ij} = 1$.

Requiring $\alpha^{ij} < 1$ is not surprising. In fact, the fulfillment of this condition requires that

$$\tau_f^{ij} > \Delta_*^{ij} \quad \text{and} \quad \tau_d^{ij} > 1 \tag{3.27}$$

The first requirement, $\tau_f^{ij} > \Delta_*^{ij}$, simply means that DoS can occasionally occur at a rate faster than the highest transmission rate of the link $\{i,j\}$. However, on the average, the frequency at which DoS can occur must be sufficiently small compared to sampling rate of the network link. Likewise, the second requirement, $\tau_d^{ij} > 1$, simply means that, on the average, the amount of DoS affecting link $\{i,j\}$ must necessarily be a fraction of the total time. PoC can be therefore regarded as an average connectivity property.

It is worth noting that in some cases consensus can be preserved even if $\alpha^{ij} \geq 1$ for certain network links. This happens whenever removing such links does not cause the graph to be disconnected. More precisely, let $\mathcal{X}$ be any set of links such that $\mathcal{G}_{\mathcal{X}} := (\mathcal{I}, \mathcal{E} \setminus \mathcal{X})$ remains connected. From the foregoing analysis, it is immediate to conclude that consensus is preserved whenever $\alpha^{ij} < 1$ for all $\{i,j\} \in \mathcal{E} \setminus \mathcal{X}$, even if communication over the links $\{i,j\} \in \mathcal{X}$ is permanently denied.

3.4.2 COMPARISON WITH CLASSIC CONNECTIVITY CONDITIONS

As previously noted, PoC can be regarded as an average connectivity property as it does not require graph connectivity point-wise in time. In this sense, it is reminiscent of *Persistency-of-Excitation* conditions that are found in the literature on consensus under switching topologies (*e.g.*, see Arcak (2007)). There are, however, noticeable differences. To see this, consider the simple situation in which the DoS pattern is the same for all the links, *i.e.*, $(h_n^{ij}, \tau_n^{ij}) = (h_n, \tau_n)$

for all $\{i,j\} \in \mathcal{E}$ and all $n \in \mathbb{Z}_{\geq 0}$. Under such circumstances, the incidence matrix of the graph is a time-varying matrix satisfying: i) $\mathcal{B}(t) = 0$ in the presence of DoS; and ii) $\mathcal{B}(t) = \mathcal{B}$ in the absence of DoS, where $\mathcal{B}$ represents the incidence matrix related to the nominal graph configuration. Consider now a DoS pattern consisting of countable number of singletons, *i.e.*, $H_n = \{h_n\}$ for all $n \in \mathbb{Z}_{\geq 0}$. In a classic continuous-time setting, such a DoS pattern does not destroy consensus. In fact, it is trivial to conclude that there exist constants $c_1, c_2 \in \mathbb{R}_{>0}$ such that (*cf.* Arcak (2007))

$$\int_{t_0}^{t_0+c_1} Q\mathcal{B}(t)\mathcal{B}^\top(t)Q^\top dt = Q\mathcal{B}\mathcal{B}^\top Q^\top c_1 > c_2 I \tag{3.28}$$

for all $t_0 \in \mathbb{R}_{\geq 0}$, where Q is a suitable projection matrix such that $Q\mathcal{B}(t)\mathcal{B}^\top(t)Q^\top$ is nonsingular if and only if the graph induced by $D(t)$ is connected. In the present case, in accordance with the previous discussion, consensus can instead be destroyed. The subtle, yet important, difference is due to the constraint on the frequency of the information exchange that is imposed by the network. In this sense, the notion of PoC naturally extends the Persistency-of-Excitation condition to digital networked settings by requiring that the graph connectivity be established over periods of time that are consistent with the maximum transmission rate imposed by the communication protocol.

3.4.3 ACCOUNTING FOR GENUINE DOS

In the foregoing analysis, we focused on the case where DoS is caused by malicious attacks. Of course, DoS might also result from a "genuine" network congestion. Hereafter, we will briefly discuss how the case of genuine DoS can be incorporated into the present framework. We shall focus on a deterministic formulation of the problem. A probabilistic characterization of the problem, though restricted to a centralized setting, has been proposed in Cetinkaya et al. (2015).

Let $\beta^{ij} \in [0,1]$ be an upperbound on the average percentage of transmission failures that can occur over the link $\{i,j\}$. This bound can be chosen as representative of the situation where all the network nodes exchange information at the highest transmission rate (according to (3.14), this is equal to $4d_{\max}/\varepsilon$ for each link). Here. by "average" we mean that, denoting by $T_A^{ij}(\tau,t)$ and $T_F^{ij}(\tau,t)$ the number of transmission attempts and transmission failures for the link $\{i,j\}$ on the interval $[\tau, t]$, it holds that

$$\frac{T_F^{ij}(\tau,t)}{T_A^{ij}(\tau,t)} \leq \beta^{ij} \tag{3.29}$$

as $T_A^{ij}(\tau,t) \to \infty$.

This condition can be suitably rearranged. To this end, first notice that the above condition is equivalent to the existence of a positive constant a^{ij} such that

$$T_F^{ij}(\tau,t) \leq a^{ij} + \beta^{ij} T_A^{ij}(\tau,t) \tag{3.30}$$

for all $t, \tau \in \mathbb{R}_{\geq 0}$ with $t \geq \tau$. Moreover, it holds that $T_A^{ij}(\tau,t) \leq \lceil (t-\tau)/\Delta_*^{ij} \rceil$ since, by construction, Δ_*^{ij} is the smallest inter-transmission time for the link $\{i,j\}$. Letting $b^{ij} := a^{ij} + 1$, we then have

$$T_F^{ij}(\tau,t) \leq b^{ij} + \frac{t-\tau}{(\Delta_*^{ij}/\beta^{ij})} \tag{3.31}$$

Therefore, we can regard genuine transmission failures as the result of a DoS signal in the form of a train of pulses that are superimposed to the transmission instants, where $T_F^{ij}(\tau,t)$ coincides with the number $n^{ij}(\tau,t)$ of DoS off/on transitions occurring on the interval $[\tau,t]$. Thus, Assumption 3.1 and 3.2 are satisfied with $(\mu^{ij}, \kappa^{ij}, \tau_f^{ij}, \tau_d^{ij}) = (b^{ij}, 0, \Delta_*^{ij}/\beta^{ij}, \infty)$. According to the analysis of Section 3.3, one can conclude the following: i) if only genuine transmission failures are present (no malicious DoS), Persistency-of-Communication is preserved as long as

$$\frac{1}{\tau_d^{ij}} + \frac{\Delta_*^{ij}}{\tau_f^{ij}} = \beta^{ij} < 1 \tag{3.32}$$

This is consistent with intuition and, in fact, simply means that communication over the link $\{i,j\}$ is not permanently destroyed if and only if $T_F^{ij}(\tau,t) < T_A^{ij}(\tau,t)$ on the average; ii) in case of genuine and malicious transmission failures, one can simply consider two independent DoS signals acting on the same link, each one characterized by its own 4-tuple $(\mu^{ij}, \kappa^{ij}, \tau_f^{ij}, \tau_d^{ij})$. It is immediate to see that

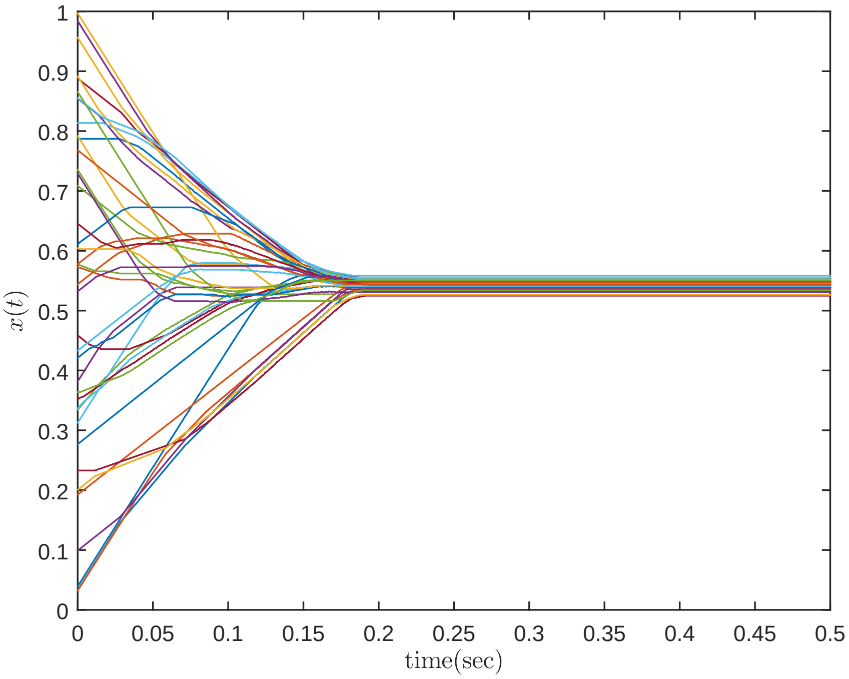

Figure 3.2: Evolution of x, corresponding to the solution to (3.2) and (3.13) for a random graph with $n = 40$ nodes in the absence of DoS.

that the analysis of Section 3.3 carries over to the present case by replacing condition $\alpha^{ij} < 1$ with $\alpha^{ij} + \beta^{ij} < 1$.

3.5 A NUMERICAL EXAMPLE

We consider a random connected undirected graph with $n = 40$ nodes and with $d^i = 4$ for all $i \in \mathcal{I}$. Nodes and control initial values are generated randomly within the interval $[0, 1]$ and the set $\{-1, 0, 1\}$, respectively.

We consider the behavior of (3.2) and (3.13) with $\varepsilon = 0.005$. Figure 3.2 depicts simulation results for the nominal case in which DoS is absent. Notice that in this case (3.13) coincides with (3.4). We next consider the case in which DoS is present. Simulation results are reported in Figure 3.3. In the simulation, we considered DoS attacks which affect each of the network links independently.

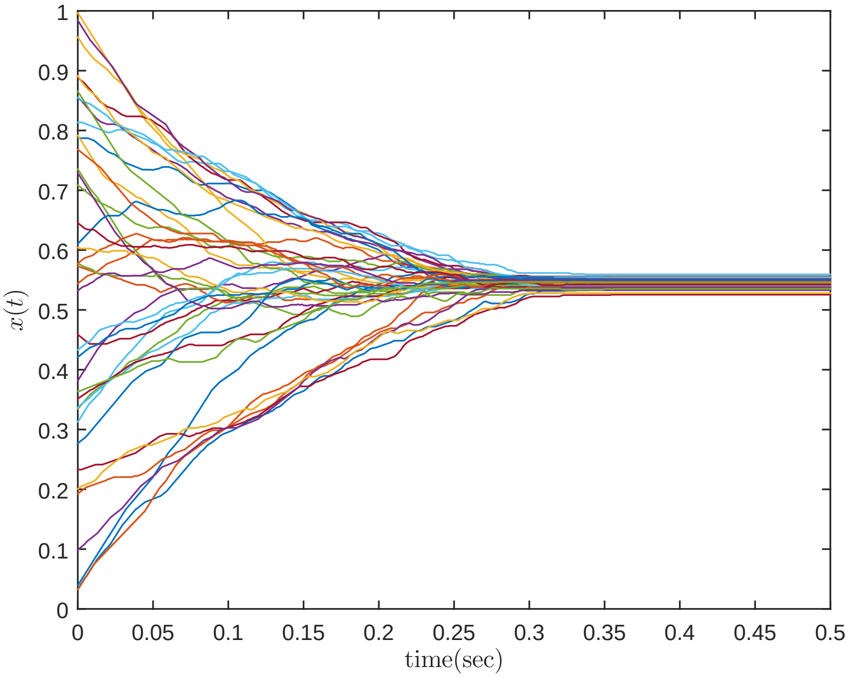

Figure 3.3: Evolution of x, corresponding to the solution to (3.2) and (3.13) for a random graph with $n = 40$ nodes in the presence of DoS.

For each link, the corresponding DoS pattern takes the form of a pulse-width modulated signal with variable period and duty cycle (maximum period of 0.15sec and maximum duty cycle equal to 100%), both generated randomly. These patterns are reported in Table I and depicted in Figure 3.4 for a few number of network links. Notice that, for each DoS pattern, one can compute corresponding values for $(\mu^{ij}, \kappa^{ij}, \tau_f^{ij}, \tau_d^{ij})$. They can be determined by computing the values $n^{ij}(\tau, t)$ and $|\Xi^{ij}(\tau, t)|$ of each DoS pattern (*cf.* Assumption 3.1 and 3.2) over the considered simulation horizon. Figure 3.5 depicts the obtained values of τ_f^{ij} and τ_d^{ij} for each $\{i, j\} \in \mathcal{E}$. One sees that these values are consistent with the requirements imposed by the PoC condition.

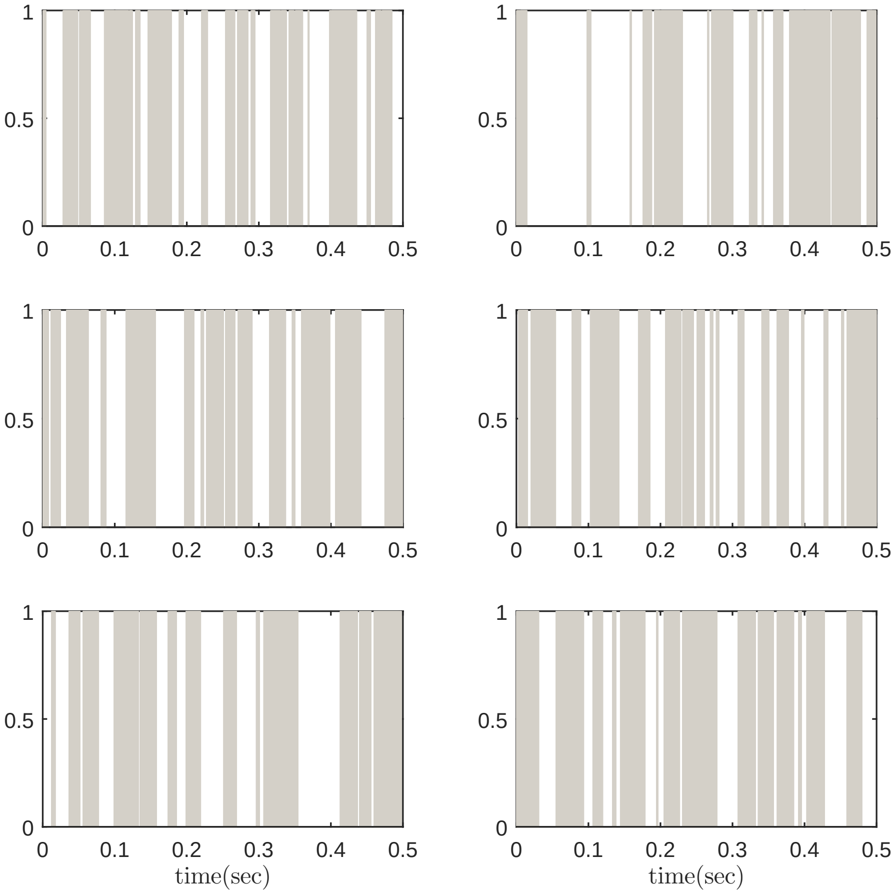

Figure 3.4: DoS pattern for the network links $\{13,14\}$, $\{6,34\}$, $\{34,39\}$, $\{9,26\}$, $\{9,21\}$ and $\{33,38\}$. The vertical gray stripes represent the time-intervals over which DoS is active.

Table 3.1: DoS average duty cycle over some links

Link $\{i,j\}$	Duty cycle (%)	Link $\{i,j\}$	Duty cycle (%)
$\{13,14\}$	49 %	$\{6,34\}$	44.78 %
$\{34,39\}$	55.96 %	$\{9,26\}$	47.3 %
$\{9,21\}$	52.76 %	$\{33,38\}$	58.96 %

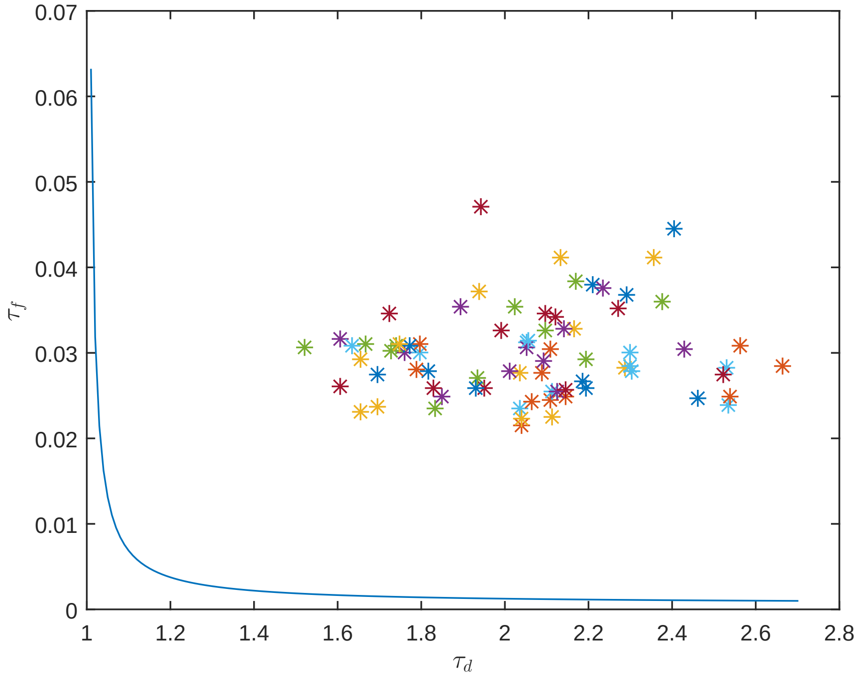

Figure 3.5: Locus of the points $1/\tau_d + \Delta_*/\tau_f^{ij} = 1$ as a function of (τ_d, τ_f) with $\Delta_* = 6.25 \times 10^{-4}$ (blue solid line). Notice that $\Delta_* = \Delta_*^{ij}$ for all $\{i, j\} \in \mathcal{E}$, so that the locus of point does not vary with $\{i, j\}$. The various $*$ represent the values of $(\tau_d^{ij}, \tau_f^{ij})$ for the network links.

In order to further substantiate the performance of the proposed resilient coordination protocol, we consider a larger connected and undirected network comprised of $n = 100$ nodes where each nodes is randomly connected to 6 neighbors, i.e. $d^i = 6$. The coordination parameters are as before. The simulation results for the new example in the presence and absence of DoS are given in Figure 3.6 and Figure 3.7, respectively.

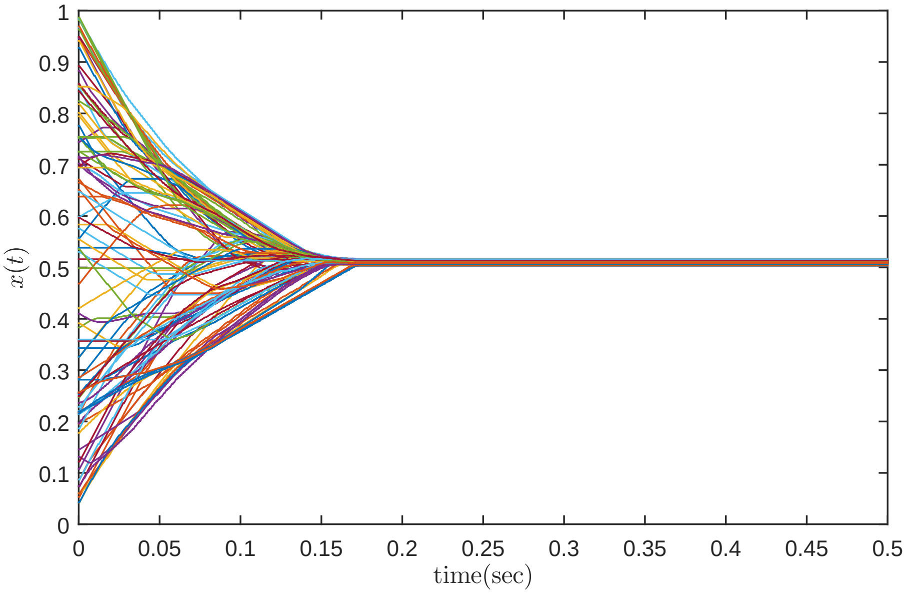

Figure 3.6: Evolution of state x in the absence of DoS.

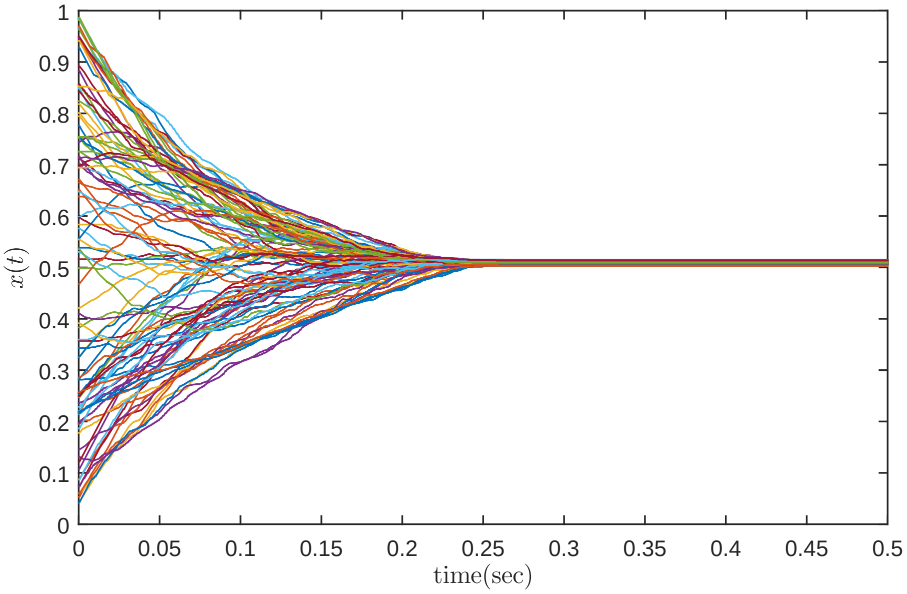

Figure 3.7: Evolution of state x in the presence of DoS.

4

Synchronization of Self-triggered Networks under Jamming

ABSTRACT

In this chapter, we investigate self-triggered synchronization of linear oscillators in the presence of communication failures caused by Denial-of-Service (DoS), thus extending the previous analysis to networks involving high-order dynamics. In line with chapter 3, a general framework is considered in which network links can fail independent of each other. A characterization of DoS frequency and duration to preserve network synchronization is provided, along with an explicit characterization of the effect of DoS on the time required to achieve synchronization. An numerical example is given to substantiate the analysis.

Published as:

D. Senejohnny, P. Tesi, and C. De Persis, "Resilient self-triggered network synchronization," in *Decision and Control (CDC), 2016 IEEE 55th Conference on*. IEEE, 2016, pp. 489–494.

D. Senejohnny, P. Tesi, and C. De Persis, "Resilient self-triggered network synchronization," in *Control Subject to Computational and Communication Constraints*, S. Tarbouriech, A. Girard, and L. Hetel, Eds. Springer International Publishing, 2018, ch. 11.

Notation: The following notations are employed throughout this chapter. The Z dimensional identity matrix is denoted by I_Z. Vectors of all ones and zeros are denoted by $\mathbb{1}$ and $\mathbb{0}$, respectively. In this chapter, the stacking of n column vectors $x_1, x_2, \ldots, x_n$, where $x_i \in \mathbb{R}^N$, is denoted by

$$x := \begin{bmatrix} x_1^\top & x_2^\top & \ldots & x_n^\top \end{bmatrix}^\top$$

where $x \in \mathbb{R}^{nN}$. Furthermore, the ℓ-th component of vector x is denoted by x_ℓ or, interchangeably, by $[x]_\ell$.

4.1 SELF-TRIGGERED SYNCHRONIZATION

4.1.1 SYSTEM DEFINITION

We consider a connected and undirected graph $\mathcal{G} = (\mathcal{I}, \mathcal{E})$, where $\mathcal{I} := \{1, 2, \cdots, n\}$ is the set of nodes and $\mathcal{E} \subseteq \mathcal{I} \times \mathcal{I}$ is the set of links (edges). Given a node $i \in \mathcal{I}$, we shall denote by $\mathcal{N}_i = \{j \in \mathcal{I} : (i,j) \in \mathcal{E}\}$ the set of its neighbors, *i.e.*, the set of nodes that exchange information with node i, and by $d^i = |\mathcal{Q}_i|$, *i.e.*, the cardinality of $\mathcal{Q}_i$. Notice that the order of the elements i and j in (i,j) is irrelevant since the graph is assumed undirected. Throughout the chapter, we shall refer to $\mathcal{G}$ as the "nominal" network (the network configuration when communication is allowed for every link).

We assume that each network node is a dynamical system consisting of a linear oscillator with dynamics

$$\dot{x}^i = Ax^i + Bu^i \tag{4.1}$$

where (A, B) is a stablizable pair and all eigenvalues of A lie on imaginary axis with unitary geometric multiplicity; $x^i, u^i \in \mathbb{R}^N$ represent node state and control variables. The network nodes exchange information according to the configuration described by the links of $\mathcal{G}$. To achieve synchronization with constrained flow of information, we employ a hybrid controller with state variables $(x, \eta, \xi, \theta) \in \mathbb{R}^{nN} \times \mathbb{R}^{nN} \times \mathbb{R}^{nd} \times \mathbb{R}^{nd}$, where $d := \sum_{i=1}^N d^i$. The controller makes use of a quantization function.

The specific quantizer of choice is $\operatorname{sign}_\varepsilon : \mathbb{R} \to \{-1, 0, 1\}$, which is given by

$$\operatorname{sign}_\varepsilon(z) := \begin{cases} \operatorname{sign}(z) & \text{if } |z| \geq \varepsilon \\ 0 & \text{otherwise} \end{cases} \tag{4.2}$$

where $\varepsilon > 0$ is a sensitivity parameter, which is selected at the design stage to trade-off between synchronization accuracy and communication frequency. The flow dynamics are given by

$$\dot{\eta}^i = (A + BK)\eta^i + \sum_{j \in \mathcal{N}_i} \xi^{ij} \tag{4.3a}$$

$$\dot{\xi}^{ij} = A\xi^{ij} \tag{4.3b}$$

$$\dot{\theta}^{ij} = -\mathbb{1} \tag{4.3c}$$

$$u^i = K\eta^i \tag{4.3d}$$

where $A + KB$ is Hurwitz; $\eta^i \in \mathbb{R}^N$ and $\xi^{ij} \in \mathbb{R}^N$ are controller states, and $\theta^{ij} \in \mathbb{R}^N$ is the local clock over the link $(i, j) \in \mathcal{E}$, where $\theta^{ij}(0) = 0$. As it will become clear in the sequel, the superscript "ij" appearing in ξ and θ indicates that these variables are common to nodes i and j. The continuous evolution of the edge-based controller dynamic holds as long as the set

$$\mathcal{S}(\theta, t) := \{(i, j, \ell) \in \mathcal{I} \times \mathcal{I} \times \mathcal{L}^* : \theta^{ij}_\ell(t^-) = 0\} \tag{4.4}$$

is non-empty, where $s(t^-)$ denotes the limit from below of a signal $s(t)$, *i.e.*, $s(t^-) = \lim_{\tau \nearrow t} s(\tau)$, and where $\ell \in \mathcal{L}^* := \{1, 2, \dots, N\}$. At these time instants, in the "nominal" operating mode, a discrete transition (jump) occurs, which is given by

$$\begin{aligned}
x^i_\ell(t) &= x^i_\ell(t^-) \\
\eta^i_\ell(t) &= \eta^i_\ell(t^-) \\
\xi^{ij}_\ell(t) &= \begin{cases} [e^{At}\,\mathrm{sign}_\varepsilon(e^{-At}\mathcal{D}^{ij}(\eta(t) - x(t)))]_\ell & \text{if } (i, j, \ell) \in \mathcal{S}(\theta, t) \\ \xi^{ij}_\ell(t^-) & \text{otherwise} \end{cases} \\
\theta^{ij}_\ell(t) &= \begin{cases} f^{ij}_\ell(t) & \text{if } (i, j, \ell) \in \mathcal{S}(\theta, t) \\ \theta^{ij}_\ell(t^-) & \text{otherwise} \end{cases}
\end{aligned} \tag{4.5}$$

for every $i \in \mathcal{I}$, $j \in \mathcal{N}_i$ and $\ell \in \mathcal{L}^*$.

Here, $\mathcal{D}^{ij}(\alpha(t)) = \alpha^j(t) - \alpha^i(t)$ and $f^{ij}_\ell : \mathbb{R}^n \to \mathbb{R}_{>0}$ is given by

$$f^{ij}_\ell(x) = \max\left\{ \frac{\left|\left[e^{-At}\mathcal{D}^{ij}(\eta(t) - x(t))\right]_\ell\right|}{2(d^i + d^j)}, \frac{\varepsilon}{2(d^i + d^j)} \right\} \tag{4.6}$$

Note that for all $(i,j) \in \mathcal{E}$ we have $\theta^{ij}(t) = \theta^{ji}(t)$ and $\xi^{ij}(t) = -\xi^{ji}(t)$ for all $t \in \mathbb{R}_{\geq 0}$. As such, (4.1)-(4.5) can be regarded as an edge-based synchronization protocol. Here, the term "self-triggered", first adopted in the context of real-time systems Velasco et al. (2003), expresses the property that the data exchange between nodes is driven by local clocks, which avoids the need for a common global clock.

A few comments are in order.

Remark 4.1 (Controller structure)**.** The controller emulates the node dynamics (4.1), with an extra coupling term as done in Scardovi and Sepulchre (2009). The coupling is through the variable ξ^{ij}, which is updated at discrete times and emulates the open-loop behavior of (4.1) during its the controller continuous evolution De Persis (2013). Slightly different from Scardovi and Sepulchre (2009), the coupling term ξ^{ij} takes into account the discrepancy between node and controller states. This choice of coupling is due to the use of the quantizer (4.2) which triggers at discrete instances.

Remark 4.2 (Clock variable θ^{ij}_{ℓ})**.** Each clock variable θ^{ij}_{ℓ} plans ahead the update time of component ℓ of controller state ξ^{ij}. Whenever θ^{ij}_{ℓ} reaches zero, the ℓ-th component of the controller state and clock variables is updated. In order to avoid arbitrarily fast sampling (Zeno phenomena), we use the threshold ε in the update of the function f^{ij} in (4.6). In particular, this implies that for every edge $(i,j) \in \mathcal{E}$ and for any time $\mathcal{T}$, no more than $n\lfloor \frac{2(d^i+d^j)\mathcal{T}}{\varepsilon} + 1 \rfloor$ number of updates can occur over an interval of length $\mathcal{T}$.

4.1.2 SELF-TRIGGERED SYNCHRONIZATION

Inspired by Scardovi and Sepulchre (2009), we analyze (4.1)-(4.5) using the change of coordinates

$$\begin{aligned}
x^i(t) &= x^i(t) \\
\mathcal{X}^i(t) &= e^{-At}(\eta^i(t) - x^i(t)) \\
\mathcal{U}^{ij}(t) &= e^{-At}\xi^{ij}(t) \\
\theta^{ij}(t) &= \theta^{ij}(t)
\end{aligned} \tag{4.7}$$

Accordingly, the network state variables become $(x, \mathcal{X}, \mathcal{U}, \theta) \in \mathbb{R}^{nN} \times \mathbb{R}^{nN} \times \mathbb{R}^{nd} \times \mathbb{R}^{nd}$ with corresponding flow dynamics

$$\dot{x}^i(t) = (A + BK)x^i(t) + BKe^{At}\mathcal{X}^i(t) \tag{4.8a}$$

$$\begin{aligned} \dot{\mathcal{X}}^i(t) &= \sum_{j \in \mathcal{N}_i} \mathcal{U}^{ij} \\ \dot{\mathcal{U}}^{ij}(t) &= \mathbb{0} \\ \dot{\theta}^{ij}(t) &= -\mathbb{1} \end{aligned} \tag{4.8b}$$

and discrete transitions (jumps)

$$x^i_\ell(t) = x^i_\ell(t^-) \tag{4.9a}$$

$$\begin{aligned} \mathcal{X}^i_\ell(t) &= \mathcal{X}^i_\ell(t^-) \\ \mathcal{U}^{ij}_\ell(t) &= \begin{cases} \operatorname{sign}_\varepsilon\left(\mathcal{D}^{ij}_\ell(\mathcal{X}(t))\right) & \text{if } (i,j,\ell) \in \mathcal{S}(\theta, t) \\ \mathcal{U}^{ij}_\ell(t^-) & \text{otherwise} \end{cases} \\ \theta^{ij}_\ell(t) &= \begin{cases} g^{ij}_\ell(\mathcal{X}(t)) & \text{if } (i,j,\ell) \in \mathcal{S}(\theta, t) \\ \theta^{ij}_\ell(t^-) & \text{otherwise} \end{cases} \end{aligned} \tag{4.9b}$$

where $(i, j, \ell) \in \mathcal{I} \times \mathcal{I} \times \mathcal{L}^*$ and

$$g^{ij}_\ell(\mathcal{X}(t)) = \max\left\{ \frac{\left|\mathcal{D}^{ij}_\ell(\mathcal{X}(t))\right|}{2(d^i + d^j)}, \frac{\varepsilon}{2(d^i + d^j)} \right\} \tag{4.10}$$

Notice that the notion of local time in both coordinates is the same. The reason for considering this change of coordinates is to transform the origianl synchronization problem into a consensus problem that involves integrator variables $\mathcal{X}^i$.

The result which follows is the main result of this section.

Theorem 4.1. *Let all the eigenvalues of A lie on the imaginary axis with geometric multiplicity equal to one. Let $(x, \mathcal{X}, \mathcal{U}, \theta)$ be the solution to system* (4.8) *and* (4.9).

Then there exist a finite time T such that $\mathcal{X}$ converges within the time T to a point $\mathcal{X}_* = [\mathcal{X}_*^{1\top}, \dots, \mathcal{X}_*^{n\top}]^\top$ in the set

$$\mathcal{E} := \left\{ \mathcal{X} \in \mathbb{R}^{nN} : |\mathcal{D}_\ell^{ij}(\mathcal{X})| < \delta \quad \forall (i,j,\ell) \in \mathcal{I} \times \mathcal{I} \times \mathcal{L}^* \right\} \tag{4.11}$$

where $\delta = \varepsilon(n-1)$, and $\mathcal{U}(t) = 0$ for all $t \geq T$. Moreover, for any arbitrary small $\varepsilon_c \in \mathbb{R}_{>0}$ there exist a time $T_c(\varepsilon_c) \geq T$ such that

$$\left| x_\ell^i(t) - x_\ell^j(t) \right| < 2\varepsilon_c + \sqrt{N}\,\delta \quad \forall (i,j,\ell) \in \mathcal{I} \times \mathcal{I} \times \mathcal{L}^* \tag{4.12}$$

for all $t \geq T_c(\varepsilon_c)$, where N is the dimension of the vector x.

Proof of Theorem 4.1. As a first step, we analyze the consensus of subsystem $(\mathcal{X}, \mathcal{U}, \theta)$. Afterwards, we will investigate the synchronization of the states x^i throughout the relation $\mathcal{X}^i(t) = e^{-At}(\eta^i(t) - x^i(t))$.

Consider the Lyapunov function $V(\mathcal{X}) = \frac{1}{2}\mathcal{X}^\top \mathcal{X}$, and let $t_{\ell_k}^{ij} := \max\{t_l^{ij} : t_l^{ij} \leq t, l \in \mathbb{Z}_{\geq 0}\}$. The derivative of V along the solutions to (4.8) satisfies

$$\begin{aligned}
\dot{V}(\mathcal{X}(t)) &= \sum_{i=1}^{N} \mathcal{X}^{i\top}(t)\,\dot{\mathcal{X}}^i(t) \\
&= -\sum_{(i,j)\in\mathcal{E}} (\mathcal{X}^j(t) - \mathcal{X}^i(t))^\top \mathcal{U}^{ij}(t_{\ell_k}^{ij}) \\
&= -\sum_{(i,j)\in\mathcal{E}} \sum_{\ell=1}^{n} \mathcal{D}_\ell^{ij}(\mathcal{X}(t))\,\mathrm{sign}_\varepsilon(\mathcal{D}_\ell^{ij}(\mathcal{X}(t_{\ell_k}^{ij})))
\end{aligned} \tag{4.13}$$

During the continuous evolution $|\dot{\mathcal{D}}_\ell^{ij}(\mathcal{X}(t))| \leq d^i + d^j$ for $t \in [t_k^i, t_{k+1}^i[$, where $\mathcal{D}^{ij}(\mathcal{X}(t)) = \mathcal{X}^j(t) - \mathcal{X}^i(t)$. Exploiting this fact and recalling the definition of $g_\ell^{ij}(\mathcal{X}(t))$ in (4.10), it holds that if $|\mathcal{D}_\ell^{ij}(\mathcal{X}(t_{\ell_k}^{ij}))| \geq \varepsilon$ then

$$\begin{aligned}
|\mathcal{D}_\ell^{ij}(\mathcal{X}(t))| &\geq |\mathcal{D}_\ell^{ij}(\mathcal{X}(t_{\ell_k}^{ij}))| - (d^i + d^j)(t - t_{\ell_k}^{ij}) \\
&\geq \frac{|\mathcal{D}_\ell^{ij}(\mathcal{X}(t_{\ell_k}^{ij}))|}{2}
\end{aligned} \tag{4.14}$$

and

$$\mathrm{sign}_\varepsilon(\mathcal{D}_\ell^{ij}(\mathcal{X}(t))) = \mathrm{sign}_\varepsilon(\mathcal{D}_\ell^{ij}(\mathcal{X}(t_{\ell_k}^{ij}))) \tag{4.15}$$

Using (4.14) and (4.15) we conclude that

$$\dot{V}(\mathcal{X}(t)) \leq - \sum_{(i,j)\in\mathcal{E}} \sum_{\substack{\ell\in\mathcal{L}^*: \\ |\mathcal{D}_\ell^{ij}(\mathcal{X}(t_{\ell_k}^{ij}))|\geq\varepsilon}} \frac{|\mathcal{D}_\ell^{ij}(\mathcal{X}(t_{\ell_k}^{ij}))|}{2} \tag{4.16}$$

In view of (4.16), there must exist a finite time T such that, for every $(i,j) \in \mathcal{E}$ and every k, ℓ with $t_{\ell_k}^{ij} \geq T$, it holds that $|\mathcal{D}_\ell^{ij}(\mathcal{X}(t_{\ell_k}^{ij}))| < \varepsilon$. This is because, otherwise, V would become negative. The inequality in (4.11) follows by recalling that, in a graph with N nodes the graph diameter is $N-1$. This shows that $\mathcal{X}$ converges in a finite time T to a point $\mathcal{X}_*$ in the set $\mathcal{E}$.

We now focus on x. In view of (4.2), $\mathcal{U}$ converges to zero in a finite time. Moreover, in view of (4.7), we have that $\eta^i(t) - x^i(t)$ converges to $e^{At}\mathcal{X}_*^i$ and ξ to $\mathbb{0}$ in a finite time. As for η, recall that η^i has flow and jump dynamics given by

$$\begin{aligned} \dot{\eta}^i(t) &= (A+BK)\eta^i(t) + \sum_{j\in\mathcal{N}_i} \xi^{ij}(t) \\ \eta^i(t) &= \eta^i(t^-) \end{aligned} \tag{4.17}$$

Hence, η converges exponentially to the origin since ξ converges to $\mathbb{0}$ is a finite time and $A+BK$ is Hurwitz. Combining this fact with the property that $\eta^i(t) - x^i(t)$ convergence asymptotically to $e^{At}\mathcal{X}_*^i$, we have that $x^i(t)$ convergence asymptotically to $-e^{At}\mathcal{X}_*^i$. This implies that for any node $i \in \mathcal{I}$ and any $\varepsilon_c \in \mathbb{R}_{>0}$, there exists a time $T_c(\varepsilon_c)$ after which $\|x^i(t) + e^{At}\mathcal{X}_*^i\| \leq \varepsilon_c$, where $\|\cdot\|$ stands for Euclidean norm.

Notice that in general $\mathcal{X}_*^i \neq \mathcal{X}_*^j$ for $i \neq j$ in accordance with the approximate consensus property (4.11). Therefore, the solutions x^i and x^j for all $(i,j) \in \mathcal{I}\times\mathcal{I}$ will achieve approximate consensus as well. In particular, an upper bound on their disagreement level can be estimated as

$$\begin{aligned} \|x^i(t) - x^j(t)\| &\leq \|x^i(t) + e^{At}\mathcal{X}_*^i\| + \|x^j(t) + e^{At}\mathcal{X}_*^i\| \\ &\leq \|x^i(t) + e^{At}\mathcal{X}_*^i\| + \|x^j(t) + e^{At}\mathcal{X}_*^j\| + \|e^{At}\mathcal{X}_*^i - e^{At}\mathcal{X}_*^j\| \\ &\leq 2\varepsilon_c + \|e^{At}(\mathcal{X}_*^j - \mathcal{X}_*^i)\| \\ &\leq 2\varepsilon_c + \sqrt{n}\,\delta \end{aligned} \tag{4.18}$$

where the last inequality is obtained from (4.11) and the fact that A has purely imaginary eigenvalues by hypothesis. This concludes the proof.

Proof of Proposition 4.1. Reasoning as in the proof of Theorem 4.1, it is an easy matter to see that in the presence of DoS (4.16) modifies into

$$\dot{V}(\mathcal{X}(t)) \leq - \sum_{(i,j)\in\mathcal{E}} \sum_{\substack{\ell\in\mathcal{L}^*: \\ |\mathcal{D}_\ell^{ij}(\mathcal{X}(t_{\ell_k}^{ij}))|\geq\varepsilon \,\wedge \\ t_{\ell_k}^{ij}\in\Theta^{ij}(0,t)}} \frac{|\mathcal{D}_\ell^{ij}(\mathcal{X}(t_{\ell_k}^{ij}))|}{2} \tag{4.19}$$

In words, the derivative of V decreases whenever, for some $(i,j) \in \mathcal{E}$, $\ell \in \mathcal{L}^*$, two conditions are met: i) $|\mathcal{D}_\ell^{ij}(\mathcal{X}(t_{\ell_k}^{ij}))| \geq \varepsilon$, which means that i and j are not component-wise ε-close; and ii) communication on the link that connects i and j is possible.

From (4.19) there must exist a finite time T_* such that, for every $\{i,j,\ell\} \in \mathcal{E}\times\mathcal{L}^*$ and every k with $t_{\ell_k}^{ij} \geq T_*$, it holds that $|\mathcal{D}_\ell^{ij}(\mathcal{X}(t_{\ell_k}^{ij}))| < \varepsilon$ or $t_{\ell_k}^{ij} \in \Xi^{ij}(0,t)$. This is because, otherwise, V would become negative. The proof follows by recalling that in both the cases $|\mathcal{D}_\ell^{ij}(\mathcal{X}(t_{\ell_k}^{ij}))| < \varepsilon$ and $t_{\ell_k}^{ij} \in \Xi^{ij}(0,t)$ the control $\mathcal{U}_\ell^{ij}(t)$ is set equal to zero.

Proof of Proposition 4.2. Consider any link $(i,j) \in \mathcal{E}$, and suppose that a certain transmission attempt $t_{\ell_k}^{ij}$ is unsuccessful. We claim that a successful transmission over the link (i,j) does always occur within $[t_{\ell_k}^{ij}, t_{\ell_k}^{ij} + \Phi^{ij}]$. We prove the claim by contradiction. To this end, we first introduce a number of auxiliary quantities. Denote by $\bar{H}_n^{ij} := \{h_n^{ij}\} \cup [h_n^{ij}, h_n^{ij} + \tau_n^{ij} + \Delta_*^{ij}[$. the n-th DoS interval over the link (i,j) prolonged by Δ_*^{ij} units of time. Also, let

$$\bar{\Xi}^{ij}(\tau,t) := \bigcup_{n\in\mathbb{Z}_{\geq 0}} \bar{H}_n^{ij} \bigcap [\tau,t] \tag{4.20}$$

$$\bar{\Theta}^{ij}(\tau,t) := [\tau,t] \setminus \bar{\Xi}^{ij}(\tau,t) \tag{4.21}$$

Suppose then that the claim is false, and let $t_\ell^\star$ denote the last transmission attempt over $[t_{\ell_k}^{ij}, t_{\ell_k}^{ij} + \Phi^{ij}]$. Notice that this necessarily implies $|\bar{\Theta}^{ij}(t_{\ell_k}^{ij}, t_\ell^\star)| = 0$. To see this, first note that, in accordance with (4.26), the inter-sampling time over the interval $[t_{\ell_k}^{ij}, t_\ell^\star]$ is equal to $\varepsilon/(2(d^i + d^j)) = \Delta_*^{ij}$. Hence, we cannot have $|\bar{\Theta}^{ij}(t_{\ell_k}^{ij}, t_\ell^\star)| > 0$ since this would imply the existence of a DoS-free interval within $[t_{\ell_k}^{ij}, t_\ell^\star]$ of length greater than Δ_*^{ij}, which is not possible since, by hypothesis, no successful transmission attempt occurs within $[t_{\ell_k}^{ij}, t_\ell^\star]$. Thus $|\bar{\Theta}^{ij}(t_{\ell_k}^{ij}, t_\ell^\star)| = 0$. Moreover, since $t_\ell^\star$ is unsuccessful, it must be contained in a DoS interval, say H_q^{ij}. This implies $[t_\ell^\star, t_\ell^\star + \Delta_*^{ij}[\subseteq \bar{H}_q^{ij}$. Hence, we have

$$\begin{aligned} |\bar{\Theta}^{ij}(t_{\ell_k}^{ij}, t_\ell^\star + \Delta_*^{ij})| &= |\bar{\Theta}^{ij}(t_{\ell_k}^{ij}, t_\ell^\star)| + |\bar{\Theta}^{ij}(t_\ell^\star, t_\ell^\star + \Delta_*^{ij})| \\ &= 0 \end{aligned} \tag{4.22}$$

However, condition $|\bar{\Theta}(t_{\ell_k}^{ij}, t_\ell^\star + \Delta_*^{ij})| = 0$ is not possible. To see this, notice that

$$\begin{aligned} |\bar{\Theta}^{ij}(t_{\ell_k}^{ij}, t)| &= t - t_{\ell_k}^{ij} - |\bar{\Xi}^{ij}(t_{\ell_k}^{ij}, t)| \\ &\geq t - t_{\ell_k}^{ij} - |\Xi^{ij}(t_{\ell_k}^{ij}, t)| - (n(t_{\ell_k}^{ij}, t) + 1)\Delta_*^{ij} \\ &\geq (t - t_{\ell_k}^{ij})(1 - \alpha^{ij}) - \kappa^{ij} - (\mu^{ij} + 1)\Delta_*^{ij} \end{aligned} \tag{4.23}$$

for all $t \geq t_{\ell_k}^{ij}$ where the first inequality follows from the definition of the set $\bar{\Xi}^{ij}(\tau, t)$ while the second one follows from Assumption 4.1 and 4.2. Hence, by (4.23), we have $|\bar{\Theta}^{ij}(t_{\ell_k}^{ij}, t)| > 0$ for all $t > t_{\ell_k}^{ij} + (1-\alpha^{ij})^{-1}(\kappa^{ij} + (\mu^{ij}+1)\Delta_*^{ij}) = t_{\ell_k}^{ij} + \Phi^{ij}$. Accordingly, $|\bar{\Theta}(t_{\ell_k}^{ij}, t_\ell^\star + \Delta_*^{ij})| = 0$ cannot occur because $t_\ell^\star + \Delta_*^{ij} > t_{\ell_k}^{ij} + \Phi^{ij}$. In fact, by hypothesis, $t_\ell^\star$ is defined as the last unsuccessful transmission attempt within $[t_{\ell_k}^{ij}, t_{\ell_k}^{ij} + \Phi^{ij}]$, and, by (4.26), the next transmission attempt after $t_\ell^\star$ occurs at time $t_\ell^\star + \Delta_*^{ij}$. This concludes the proof.

Equations (4.11) and (4.12) involve a notion of "approximate" synchronization. This amounts to saying that the solutions eventually synchronize up to an error, which can be made as small as desired by reducing ε (at the expense of an increase in the communication cost since, in view of (4.6), the minimum intertransmission time decreases with ε). Theorem 4.1 will be used as a reference frame for the analysis of Section 4.3. The case of asymptotic synchronization can be pursued along the lines of De Persis and Frasca (2013).

4.2 NETWORK DENIAL-OF-SERVICE

We shall refer to Denial-of-Service (DoS) as the phenomenon by which communication between the network nodes is interrupted. Similar to chapter 3 we consider the very general scenario in which the network communication links can fail independent of each other. The similar DoS characterization, assumption, and discussion in section 3.2 are valid in this chapter as well. For the sake of simplicity of the reader, however, the assumptions are provided once again.

Assumption 4.1 (DoS frequency)**.** *For each $(i,j) \in \mathcal{E}$, there exist $\mu^{ij} \in \mathbb{R}_{\geq 0}$ and $\tau_f^{ij} \in \mathbb{R}_{>0}$ such that*

$$n^{ij}(\tau,t) \leq \mu^{ij} + \frac{t-\tau}{\tau_f^{ij}} \tag{4.24}$$

for all $t, \tau \in \mathbb{R}_{\geq 0}$ with $t \geq \tau$.

Assumption 4.2 (DoS duration)**.** *For each $(i,j) \in \mathcal{E}$, there exist $\kappa^{ij} \in \mathbb{R}_{\geq 0}$ and $\tau_d^{ij} \in \mathbb{R}_{>1}$ such that*

$$|\Xi^{ij}(\tau,t)| \leq \kappa^{ij} + \frac{t-\tau}{\tau_d^{ij}} \tag{4.25}$$

for all $t, \tau \in \mathbb{R}_{\geq 0}$ with $t \geq \tau$.

4.3 MAIN RESULT

4.3.1 RESILIENT SELF-TRIGGERED SYNCHRONIZATION

When DoS disrupts link communications, the former controller state ξ_ℓ^{ij} is not available any more. In order to compensate for the communication failures, the control action is suitably modified as follows during the controller discrete updates,

$$
\begin{aligned}
&x^i_\ell(t) = x^i_\ell(t^-)\\
&\mathcal{X}^i_\ell(t) = \mathcal{X}^i_\ell(t^-)\\
&\mathcal{U}^{ij}_\ell(t) = \begin{cases} \operatorname{sign}_\varepsilon\left(\mathcal{D}^{ij}_\ell(\mathcal{X})\right) & \text{if } (i,j,\ell) \in \mathcal{S}(\theta,t) \wedge t \in \Theta^{ij}(0,t) \\ 0 & \text{if } (i,j,\ell) \in \mathcal{S}(\theta,t) \wedge t \in \Xi^{ij}(0,t) \\ \mathcal{U}^{ij}_\ell(t^-) & \text{otherwise} \end{cases}\\
&\theta^{ij}_\ell(t) = \begin{cases} g^{ij}_\ell(t) & \text{if } (i,j,\ell) \in \mathcal{S}(\theta,t) \wedge t \in \Theta^{ij}(0,t) \\ \dfrac{\varepsilon}{2(d^i+d^j)} & \text{if } (i,j,\ell) \in \mathcal{S}(\theta,t) \wedge t \in \Xi^{ij}(0,t) \\ \theta^{ij}_\ell(t^-) & \text{otherwise} \end{cases}
\end{aligned}
\tag{4.26}
$$

In words, the control action $\mathcal{U}^{ij}$ is reset to zero whenever the link (i,j) is in DoS status [1]. In addition to $\mathcal{U}$, also the local clocks are modified upon DoS, yielding a *two-mode* sampling logic. Let $\{t^{ij}_{\ell_k}\}_{\ell_k \in \mathbb{Z}_{\geq 0}}$ denote the sequence of transmission attempts for ℓ-th component of ξ^{ij} over the link $(i,j) \in \mathcal{E}$. Then when a communication attempt is successful $t^{ij}_{\ell_{k+1}} = t^{ij}_{\ell_k} + g^{ij}_\ell(t)$, and when it is unsuccessful $t^{ij}_{\ell_{k+1}} = t^{ij}_{\ell_k} + \varepsilon/(2(d^i+d^j))$.

In order to characterize the overall network behavior in the presence of DoS. The analysis is subdivided into two main steps: i) we first prove that all the edge-based controllers eventually stop updating their local controls; and ii) we then provide conditions on the DoS frequency and duration such that synchronization, in the sense of (4.12), is preserved. This is achieved by resorting to a notion of Persistency-of-Communication (PoC), which naturally extends the PoE condition Arcak (2007) to a digital networked setting by requiring graph connectivity over periods of time that are consistent with the constraints imposed by the communication medium.

As for i), we have the following result.

Proposition 4.1. (Convergence of the solutions*) Let* $(x, \mathcal{X}, \mathcal{U}, \theta)$ *be the solutions to* (4.8) *and* (4.26)*. Then, there exists a finite time* T_* *such that, for any* $(i,j) \in \mathcal{E}$*, it holds that* $\mathcal{U}^{ij}_\ell(t) = 0$ *for all* $\ell \in \mathcal{L}^*$ *and for all* $t \geq T_*$.

[1] Notice that this requires that the nodes are able to detect the occurrence of DoS. This is the case, for instance, with transmitters employing carrier sensing as medium access policy. Another example is when transceivers use TCP-like protocols.

Proof: See the appendix.

The above result does not allow one to conclude anything about the final disagreement vector in the sense that given a pair of nodes (i, j), the asymptotic value of $|\mathcal{X}^j_\ell(t) - \mathcal{X}^i_\ell(t)|$ and/or $|x^j_\ell(t) - x^i_\ell(t)|$ can be arbitrarily large. As an example, if node i is never allowed to communicate then $\mathcal{X}^i(t) = \mathcal{X}^i(0)$ and the oscillator state $x^i(t)$ satisfies $\dot{x}^i(t) = Ax^i(t)$ with initial condition $-\mathcal{X}^i(0)$ for all $t \in \mathbb{R}_{\geq 0}$. In order to recover the same conclusions as in Theorem 4.1, bounds on DoS frequency and duration have to be enforced. The result which follows provides one such characterization. Let $(i, j) \in \mathcal{E}$ be a generic network link, and consider a DoS sequence on (i, j), which satisfies Assumption 4.1 and 4.2. Define

$$\alpha^{ij} := \frac{1}{\tau^{ij}_d} + \frac{\Delta^{ij}_*}{\tau^{ij}_f} \tag{4.27}$$

where

$$\Delta^{ij}_* := \frac{\varepsilon}{2(d^i + d^j)} \tag{4.28}$$

As for ii), we have the following result.

Proposition 4.2 (Persistency-of-Communication (PoC))**.** *Consider any link $(i, j) \in \mathcal{E}$ employing the transmission protocol* (4.26)*. Also consider any DoS sequence on (i, j), which satisfies Assumption 4.1 and 4.2 with μ^{ij} and κ^{ij} arbitrary, and τ^{ij}_d and τ^{ij}_f such that $\alpha^{ij} < 1$. Let*

$$\Phi^{ij} := \frac{\kappa^{ij} + (\mu^{ij} + 1)\Delta^{ij}_*}{1 - \alpha^{ij}} \tag{4.29}$$

Then, for any given unsuccessful transmission attempt $t^{ij}_{\ell_k}$, at least one successful transmission occurs over the link (i, j) within the interval $[t^{ij}_{\ell_k}, t^{ij}_{\ell_k} + \Phi^{ij}]$.

Proof: See the appendix.

The following result extends the conclusions of Theorem 4.1 to the presence of DoS.

Theorem 4.2. *Let $(x, \mathcal{X}, \mathcal{U}, \theta)$ be the solution to* (4.8) *and* (4.26)*. For each $(i, j) \in \mathcal{E}$, consider any DoS sequence that satisfies Assumption 4.1 and 4.2 with η^{ij} and κ^{ij} arbitrary, and τ_d^{ij} and τ_f^{ij} such that $\alpha^{ij} < 1$. Then, $\mathcal{X}$ converges in a finite time T_* to a point $\mathcal{X}^*$ in (4.11), and $\mathcal{U}(t) = 0$ for all $t \geq T_*$. Moreover, for every $\varepsilon_c \in \mathbb{R}_{>0}$ there exist a time $T_c(\varepsilon_c) \geq T_*$ such that* (4.12) *is satisfied for all $t \geq T_c(\varepsilon_c)$.*

Proof. By Proposition 4.1, all the local controls become zero in a finite time T_*. In turn, Proposition 4.2 excludes that this is due to the persistence of a DoS status. Then the result follows along the same lines as in Theorem 4.1.

Remark 4.3. One main reason for considering DoS comes from studying network coordination problems in the presence of possibly malicious attacks. In fact, the proposed modeling framework allows to consider DoS patterns that need not follow a given class of probability distribution, which is instead a common hypothesis when dealing with "genuine" DoS phenomena such as network congestion or communication errors due to low-quality channels. In this respect, Senejohnny et al. (2017) discusses how genuine DoS can be incorporated into this modeling framework.

4.3.2 EFFECT OF DOS ON THE SYNCHRONIZATION TIME

By Theorem 4.2, $\dot{\mathcal{X}}$ becomes zero in a finite time T_* after which the network states x exponentially synchronize. Thus, it is of interest to characterize T_*, which amounts to characterizing the effect of DoS on the time needed to achieve synchronization.

Lemma 4.1 (Bound on the convergence time)**.** *Consider the same assumptions as in Theorem 4.2. Then,*

$$T_* \leq \left[\frac{1}{\varepsilon} + \frac{d_{\max}}{\varepsilon d_{\min}} + \frac{4 d_{\max}}{\varepsilon^2}\Phi\right] \sum_{i \in \mathcal{I}} \sum_{\ell \in \mathcal{L}^*} (\eta_\ell^i(0) - x_\ell^i(0))^2 \tag{4.30}$$

where $d_{\min} := \min_{i \in \mathcal{I}} d^i$ and $\Phi := \max_{(i,j) \in \mathcal{E}} \Phi^{ij}$.

Proof. Consider the same Lyapunov function V as in the proof of Theorem 4.1. Notice that, by construction of the control law and the scheduling policy, for every successful transmission $t_{\ell_k}^{ij}$ characterized by $|\mathcal{D}_\ell^{ij}(\mathcal{X}(t_{\ell_k}^{ij})| \geq \varepsilon$, the function V decreases with rate not less than $\varepsilon/2$ for at least $\varepsilon/(4d_{\max})$ units of time, in which case V decreases by at least $\varepsilon^2/(8d_{\max}) =: \varepsilon_*$. Considering all the network links, such transmissions are in total no more than $\lfloor V(0)/\varepsilon_* \rfloor$ since, otherwise, the function V would become negative. Hence, it only remains to compute the time needed to have $\lfloor V(0)/\varepsilon_* \rfloor$ of such transmissions. In this respect, pick any $t_\ell^* \geq 0$ such that consensus has still not been reached on the ℓ-th component of $\mathcal{X}$. Note that we can have $\mathcal{U}_\ell^{ij}(t_\ell^*) = 0$ for all $(i,j) \in \mathcal{E}$. However, this condition can last only for a limited amount of time. In fact, if $\mathcal{U}_\ell^{ij}(t_\ell^*) = 0$ then the next transmission attempt, say l_ℓ^{ij}, over the link (i,j) and component-ℓ will necessarily occur at a time less than or equal to $t_\ell^* + \Delta_*^{ij}$ with $\Delta_*^{ij} \leq \varepsilon/(4d_{\min})$. Let $\mathcal{Q} := [t_\ell^*, t_\ell^* + \Delta_*^{ij}]$, and suppose that over $\mathcal{Q}$ some of the controls $\mathcal{U}_\ell^{ij}$ have remained equal to zero. This implies that for some $(i,j) \in \mathcal{E}$ we necessarily have that l_ℓ^{ij} is unsuccessful. This is because if $\mathcal{U}_\ell^{ij}(t) = 0$ for all $(i,j) \in \mathcal{E}$ and all $t \in \mathcal{Q}$ then $\mathcal{X}_\ell^i(t) = \mathcal{X}_\ell^i(t_\ell^*)$ for all $i \in \mathcal{I}$ and all $t \in \mathcal{Q}$. Hence, if all the l_ℓ^{ij} were successful, we should also have $\mathcal{U}_\ell^{ij}(l_\ell^{ij}) \neq 0$ for some $(i,j) \in \mathcal{E}$ since, by hypothesis, consensus is not reached at time t_ℓ^*. Hence, applying Proposition 4.2 we conclude that at least one of the controls $\mathcal{U}_\ell^{ij}$ will become non-zero before $l_\ell^{ij} + \Phi^{ij}$. As each vector component ℓ has the same Δ_*^{ij}, at least one of the control vectors $\mathcal{U}^{ij}$ will become non-zero before the same amount of time. Overall, this implies that at least one control will become nonzero before $\varepsilon/(4d_{\min}) + \Phi$ units of time have elapsed. Since t_ℓ^* is generic, we conclude that V decreases by at least ε_* every $\varepsilon/(4d_{\max}) + \varepsilon/(4d_{\min}) + \Phi$ units of time, which implies that

$$T_* \leq \left[\frac{\varepsilon}{4d_{\max}} + \frac{\varepsilon}{4d_{\min}} + \Phi \right] \frac{V(0)}{\varepsilon_*} \tag{4.31}$$

The thesis follows by recalling that $V(0)$ can be rewritten as

$$V(0) = \frac{1}{2} \sum_{i \in \mathcal{I}} \sum_{\ell \in \mathcal{L}^*} (\mathcal{X}_\ell^i(0))^2$$

.

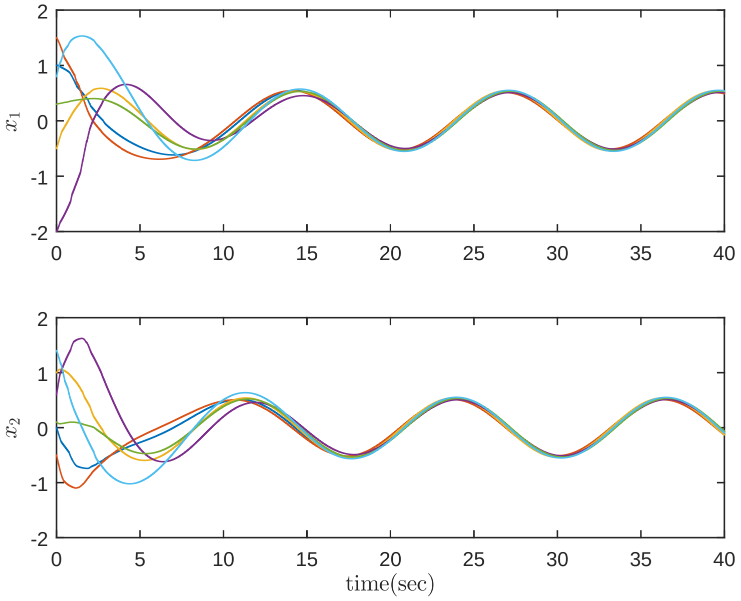

Figure 4.1: Evolution of x, corresponding to the solution to (4.1)-(4.3) and (4.26) for a random graph with $n = 6$ nodes in the presence of DoS.

4.4 A NUMERICAL EXAMPLE

We consider a random (connected) undirected graph with $n = 6$ nodes and with $d^i = 2$ for all $i \in \mathcal{I}$. Each node has linear oscillator dynamics of the form

$$\dot{x}^i(t) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} x^i(t) + \begin{bmatrix} 0 \\ 1 \end{bmatrix} u^i(t) \tag{4.32}$$

The nodes initial values are randomly within the interval $[-2, 2]$ and $(\eta(0), \xi(0), \theta(0)) = (\mathbb{0}, \mathbb{0}, \mathbb{0})$.

In the simulations, we considered DoS attacks which affect each of the network links independently. For each link, the corresponding DoS pattern takes the form of a pulse-width modulated signal with variable period and duty cycle (maximum period of 0.4 second and maximum duty cycle equal to 55%), both generated randomly. These patterns are reported in Table I for each network link.

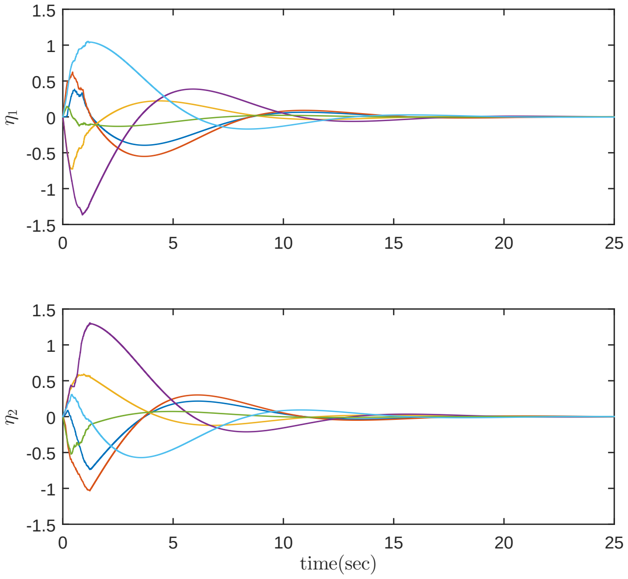

Figure 4.2: Evolution of the controller state η in the absence of DoS.

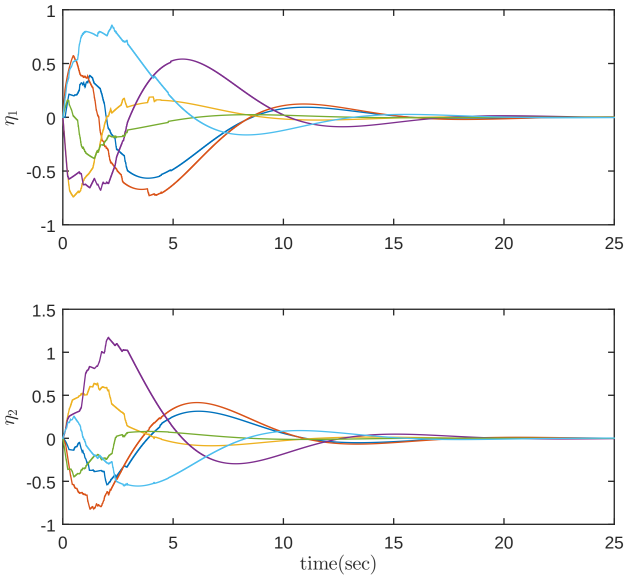

Figure 4.3: Evolution of the controller state η in the presence of DoS.

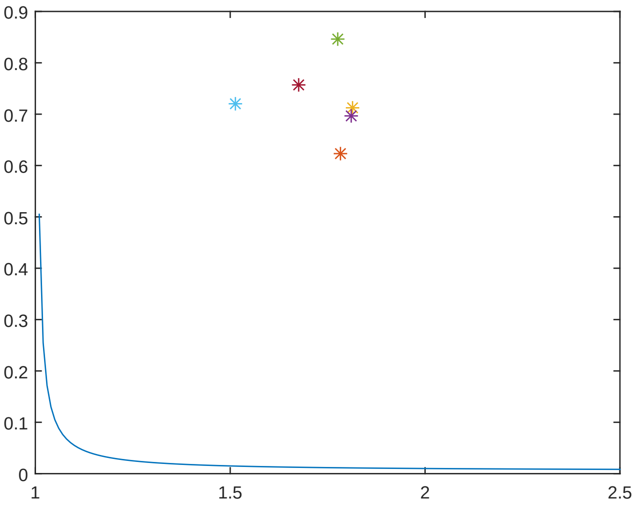

Figure 4.4: Locus of the points $1/\tau_d + \Delta_*/\tau_f^{ij} = 1$ as a function of (τ_d, τ_f) with $\Delta_* = 0.05$ (blue solid line). The horizontal axis represents τ_d and the vertical axis represents τ_f. Notice that $\Delta_* = \Delta_*^{ij}$ for all $(i,j) \in \mathcal{E}$, so that the locus of point does not vary with (i,j). The various "$*$" represent the values of $(\tau_d^{ij}, \tau_f^{ij})$ for the network links.

Table 4.1: DoS average duty cycle over links

Link (i,j)	Duty cycle (%)	Link (i,j)	Duty cycle (%)
$\{1,2\}$	56.07 %	$\{1,4\}$	55.12 %
$\{2,3\}$	55.2 %	$\{3,6\}$	56.3 %
$\{4,5\}$	66.06 %	$\{5,6\}$	59.72 %

The evolution of state $x(t)$, corresponding to the solutions to (4.1)-(4.3) and (4.26) with $\varepsilon = 0.04$ is depicted in Figure 4.1. One sees that x exhibits a quite smooth response. In fact, the impact of loss of information can be better appreciated by looking at the controller dynamics, which are reported in Figures 4.2 and 4.3. This can be explained simply by noting that the controller state ξ is affected by DoS directly while x is affected by DoS indirectly since ξ enters the node dynamics after being filtered twice.

As a final comment, note that for each DoS pattern one can compute corresponding values for $(\mu^{ij}, \kappa^{ij}, \tau_f^{ij}, \tau_d^{ij})$. They can be determined by computing $n^{ij}(\tau, t)$ and $|\Xi^{ij}(\tau, t)|$ of each DoS pattern (*cf.* Assumptions 4.1 and 4.2) over the considered simulation horizon. Figure 4.4 depicts the values obtained for τ_f^{ij} and τ_d^{ij} for each $(i, j) \in \mathcal{E}$. One sees that these values are consistent with the requirements imposed by the PoC condition.

PART II

Data Integrity Attack

Introduction

When dealing with network systems, a fundamental 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 main 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 compromise the whole network performance.

The prototypical problem to study resilience in the presence of misbehaving nodes is the so-called consensus problem (Cao et al., 2013), which forms the foundation for distributed computing. In *resilient consensus*, each node is assumed to be aware of only local information available from its neighbors and the goal is to make sure that normal nodes eventually reach a common value despite the presence of misbehaving nodes. The resilient consensus problem has a long history, and it has been investigated first by the computer scientists Dolev et al. (1986); Lynch (1996), usually under the hypothesis that the network graph is complete, that is assuming an all-to-all communication structure. More recently, thanks to the widespread of consensus-based applications, this problem has attracted a lot of interest also within the engineering community, mostly in connection with the goal of delineating the minimal connectivity assumptions that are needed to guarantee consensus.

In LeBlanc et al. (2013), the authors consider *mean subsequence reduced* (MSR) algorithms and define a graph-theoretic property, referred to as *network robustness*, which characterizes necessary and sufficient connectivity hypothesis under which normal nodes can reach consensus using only local information available from their neighbors. The results indicate that, while the communication graph should possess a certain degree of redundancy, completeness of the communication graph is not necessary even for very general types of misbehavior. The results of LeBlanc et al. (2013) have been extended in many venues. Examples include methods for handling time-varying networks Saldaña et al. (2017), double-integrator systems Dibaji and Ishii (2015), continuous-time networked systems LeBlanc and Koutsoukos (2017), sparse communication graphs with trusted nodes Abbas et al. (2014, 2017) as well as methods for identifying the robustness of specific classes of networks Usevitch and Panagou (2017).

Most of the research works in this area assume that the network operates in perfect *synchrony*, in the sense that all the nodes, at least the normal ones, update at the same moment in time. Since this condition might be difficult to obtain, a parallel line of research has focused on methods for handling *asynchrony*, which is known to render consensus much more challenging to obtain Dolev et al. (1986). Among many notable works, we mention LeBlanc and Koutsoukos (2012); Vaidya et al. (2012); Dibaji and Ishii (2017); Dibaji et al. (2017) which consider MSR-type algorithms supporting asynchrony. In these works, asynchrony refers to the property that the nodes are equipped with identical clocks, operating synchronously, but can make updates at different steps, that is at different multiples of the clock period.

The objective of this part 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. Besides the practical difficulties in achieving a perfect clock synchronization, one main reason for considering independent clocks is related to developments in the area of networked control systems where, in order to enhance efficiency and flexibility, it is more and more required to have fully autonomous devices, which is the paradigm of *event-triggered* and *self-triggered* control Heemels et al. (2012). In fact, our approach utilizes a self-triggered control scheme De Persis and Frasca (2013). Each node is equipped with a clock that determines when the next update is scheduled. At the update instant, the node polls its neighbors, collects the data and determines whether it is necessary to modify its controls along with a bound on the next update instant.

OUTLINE AND CONTRIBUTIONS

The main result of chapter 5 establishes *approximate* consensus under certain conditions on the connectivity of the communication graph and a maximum number of misbehaving nodes, conditions which can be relaxed if misbehavior only occurs in data acquisition or timing. While LeBlanc et al. (2013); LeBlanc and Koutsoukos (2012, 2017); Dibaji and Ishii (2017); Dibaji et al. (2017) achieve perfect consensus and require milder connectivity conditions, they all require the existence of a global clock that synchronize all the operations.

The present results indicate that the resilient consensus problem can be approached without requiring that the nodes are equipped with identical clocks, even when the graph is not complete, a feature which is very appealing for networked control applications.

Chapter 6 considers a modified coordination protocol with the intent of relaxing the network connectivity requirements of chapter 5. This modified protocol aims at relaxing the network connectivity requirements by searching for exact, rather than approximate, consensus. Although the convergence analysis is not yet complete, extensive simulation studies demonstrate that the proposed protocol achieves convergence under the same connectivity assumption as in LeBlanc et al. (2013).

5

Resilience against Misbehaving Nodes in Self-triggered Networks

ABSTRACT

Network systems are one of the most active research areas in the engineering community as they feature a paradigm shift from centralized to distributed control and computation. 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 step towards the development of resilient event-triggered and self-triggered coordination protocols.

Published as:

D. Senejohnny, S. Sundaram, C. De Persis, and P. Tesi, "Resilience against misbehaving nodes in self-triggered networks," in *Decision and Control (CDC), 2018 IEEE 57th Conference on*. IEEE, 2018.

D. Senejohnny, S. Sundaram, C. De Persis, and P. Tesi, "Resilience against misbehaving nodes in asynchronous networks," *Automatica, Provisionally accepted as Brief Paper*, 2018.

5.1 SYSTEM DEFINITION AND MAIN RESULT

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 let $\mathcal{Q}_i$ denote the set of neighbors of $i \in \mathcal{I}$, and by d_i the cardinality of $\mathcal{Q}_i$, that is $d_i := |\mathcal{Q}_i|$. 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

$$\begin{cases} \dot{x}_i(t) = u_i(t) \\ z_i(t) = f_i(x_i(t)) \end{cases} \quad t \in \mathbb{R}_{\geq 0} \tag{5.1}$$

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$f_i : \mathbb{R} \to \mathbb{R}$ 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 specify later on the class of misbehaviors considered in this chapter. 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 chapter.

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 nodes that the network is expected to encounter.
- A sequence $\{t_k^i\}_{k \in \mathbb{N}}$ of time instants at which node i requests data from its neighbors, where $t_0^i \in [0, t_{init}]$ defines the first time instant at which node i becomes active and $t_{init} \in \mathbb{R}_{\geq 0}$ 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 $i \in I$ 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.

5.1.1 COORDINATION PROTOCOL

Let $\mathbb{N}$ and $\mathcal{M}$ represent the sets of normal nodes and misbehaving nodes, respectively, which are assumed to be time-invariant (Assumption 5.1). We now focus on the generic k-th round of operations for node $i \in \mathbb{N}$. This 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 $h_i : \mathbb{R} \to \mathbb{R}$, $i \in \mathcal{I}$, 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 $i \in \mathbb{N}$,

$$h_i(\chi) = \chi \quad \forall \chi \in \mathbb{R} \tag{5.2}$$

A data acquisition error means that (5.2) is not satisfied for some $\chi \in \mathbb{R}$, which represents for example a fault at the receiver.

(ii) Data transmission. For $i \in \mathbb{N}$, f_i in (5.1) satisfies

$$f_i(\chi) = \chi \quad \forall \chi \in \mathbb{R} \tag{5.3}$$

which means that a normal node makes available to the other nodes its true state value. A transmission error means that (5.3) 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 from 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 $i \in \mathbb{N}$ 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 $\underline{\mathcal{E}}_i(t)$ 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 $r \in \underline{\mathcal{E}}_i(t)$ 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 $\overline{\mathcal{E}}_i(t)$ 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 $r \in \overline{\mathcal{E}}_i(t)$ 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 $i \in \mathbb{N}$, $\mathcal{D}_i(\cdot)$ satisfies

$$\mathcal{D}_i(t) = \mathcal{Q}_i \setminus \left(\underline{\mathcal{E}}_i(t) \cup \overline{\mathcal{E}}_i(t)\right) \tag{5.4}$$

and the control action is given by

$$u_i(t) = \begin{cases} 0 & t \in [0, t_0^i) \\ \mathrm{sign}_\varepsilon(\mathrm{ave}_i(t_k^i)) & t \in [t_k^i, t_{k+1}^i) \end{cases} \tag{5.5}$$

where

$$\mathrm{ave}_i(t) := \sum_{j \in \mathcal{D}_i(t)} \left(h_i(z_j(t)) - x_i(t)\right) \tag{5.6}$$

and where, for every $\chi \in \mathbb{R}$,

$$\mathrm{sign}_\varepsilon(\chi) := \begin{cases} 0 & \text{if } |\chi| < \varepsilon \\ \mathrm{sign}(\chi) & \text{otherwise} \end{cases} \tag{5.7}$$

By convention, $\mathcal{D}_i(t) = \emptyset$ implies $\mathrm{ave}_i(t) = 0$. An error in the control logic means that (5.5) is not satisfied for some $t \in \mathbb{R}_{\geq 0}$.

Remark 5.1. From a technical viewpoint, we adopt a control logic which removes "extreme" values (as in classic MSR-type algorithms) and then form an average from a subset of the remaining values through a *quantized sign* function, which saturates the control action applied at the node. This is as an approximation of the pure (non-quantized) control law introduced in Cortés (2006), which, in the absence of misbehaving nodes, guarantees *max-min* consensus, the quantization being instrumental to avoid a continuous data flow among the nodes. Interestingly, the use of sign functions has been considered to solve consensus on the *median value* Franceschelli et al. (2017), which is inherently robust to outliers and thus to some types of misbehavior. Although our work is substantially different 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.

(iv) Timing. For $i \in \mathbb{N}$, the next round of operations is scheduled at time $t^i_{k+1} = t^i_k + \Delta^i_k$, where

$$\begin{aligned} &\Delta^i_k \geq \underline{\Delta}_i \\ &\Delta^i_k \leq \frac{1}{4d^i} \max\{\varepsilon, \, |\operatorname{ave}_i(t^i_k)|\} \end{aligned} \tag{5.8}$$

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 (5.8) is not satisfied for some $k \in \mathbb{N}$.

5.1.2 ASSUMPTIONS AND MAIN RESULTS

Assumption 5.1. *The set $\mathcal{M}$ of misbehaving nodes does not change over time and $|\mathcal{M}| \leq F$.*

Assumption 5.2. *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 $\Delta^i_k \geq \underline{\Delta}_i$ for all $k \in \mathbb{N}$ for some $\underline{\Delta}_i \in \mathbb{R}_{>0}$.*

Assumption 5.3. *Every pair of normal nodes have at least $3F + 1$ neighbors in common.*

Assumption 5.4. *Every pair of normal nodes have at least $2F + 1$ neighbors in common.*

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 5.2 entails no upper bound on Δ^i_k. This is in order to capture the event that a misbehaving node never collects data from its neighbors and applies an open-loop control.

Assumptions 5.3 and 5.4 deal with the graph connectivity properties, and their use will vary depending on the type of nodes misbehavior. Both the assumptions ensure that the normal nodes share sufficient "genuine" information for taking control decisions. These assumptions hold, for instance, for classes of *strongly regular graphs* Godsil and Royle (2001), though it is not needed that the graph is regular. These assumptions should be interpreted as design conditions when the graph topology can be assigned. Let λ denote the number of neighbors that every pair of normal node share. From the Assumptions 5.3 and 5.4, λ is either $3F+1$ or $2F+1$. Consider a complete graph of $\lambda+1$ nodes. Then add k more nodes, where each of these k nodes connects to all of the $\lambda+1$ nodes in the clique. This graph with $n = \lambda+k+1$ nodes has the property that every pair of nodes has at least λ nodes in common and we see that, for fixed F, the number of edges scales only linearly with n.

We now state the main results of the chapter, which are proven in Sections 5.3 and 5.4.

Theorem 5.1. *Consider the network system (5.1)-(5.8), with the misbehaving nodes exhibiting an error in any of the operations (i)-(iv). If Assumptions 5.1, 5.2 and 5.3 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 $i, j \in \mathbb{N}$.*

Theorem 5.2. *Consider the network system (5.1)-(5.8), with the misbehaving nodes exhibiting an error in the operation (i) and/or (iv). If Assumptions 5.1, 5.2 and 5.4 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 $i, j \in \mathbb{N}$.*

Intuitively, errors in data acquisition or timing are less critical as they do not alter control or output values.

5.2 MONOTONICITY PROPERTIES

The results of this section rely on Assumption 5.1 and 5.2 only, and are thus independent of the specific type of nodes misbehavior. Let

$$x_m(t) := \min_{i \in \mathbb{N}} x_i(t), \quad x_M(t) := \max_{i \in \mathbb{N}} x_i(t) \tag{5.9}$$

where $t \in \mathbb{R}_{\geq 0}$.

The first result shows that normal nodes remain in the convex hull containing their initial values.

Lemma 5.1. *Consider the network system (5.1)-(5.8), and let Assumptions 5.1 and 5.2 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 an index $i \in \mathbb{N}$ such that

$$\begin{cases} x_i(\tau) \leq x_j(\tau) \quad \forall j \in \mathbb{N} \\ u_i(\tau) < 0 \end{cases} \tag{5.10}$$

Clearly, there could be multiple nodes achieving (5.10) at time τ. In this case, i is any of such nodes. 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 $\mathrm{ave}_i(t_k^i) \leq -\varepsilon < 0$. 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 misbehaving nodes are not more than F by Assumption 5.1, if a misbehaving node j gives $z_j(t_k^i) < x_i(t_k^i)$ 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 (5.10), there must exist a node $s \in \mathbb{N}$ such that

$$\begin{cases} x_s(t_k^i) \leq x_j(t_k^i) \quad \forall j \in \mathbb{N} \\ x_s(t_k^i) < x_i(t_k^i) \\ x_i(\tau) \leq x_j(\tau) \quad \forall j \in \mathbb{N} \\ u_i(\tau) < 0 \end{cases} \tag{5.11}$$

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 $j \in \mathbb{N}$ only if $\tau - t^i_k \geq \beta/2$. However,

$$\begin{aligned} \Delta^i_k &\leq \frac{1}{4d^i} \sum_{j \in \mathcal{D}_i(t^i_k)} (x_i(t^i_k) - z_j(t^i_k)) \\ &\leq \frac{1}{4d^i} \sum_{j \in \mathcal{D}_i(t^i_k)} (x_i(t^i_k) - x_s(t^i_k)) \end{aligned} \tag{5.12}$$

The first equality follows from the fact that $u_i(t^i_k) < 0$ requires $\mathrm{ave}_i(t^i_k) \leq -\varepsilon$ so that $\Delta^i_k \leq |\,\mathrm{ave}_i(t^i_k)|/(4d^i)$. On the other hand, the second inequality follows since $z_j(t^i_k) < x_s(t^i_k)$ only if j is misbehaving, in which case it is discarded by node i in view of Assumption 5.1 and by the control logic. Since $|\mathcal{D}_i(t)| \leq d^i$ for all $t \in \mathbb{R}_{\geq 0}$ then $\Delta^i_k \leq \beta/4$. This leads to a contradiction since it implies $\beta/2 \leq \tau - t^i_k < \Delta^i_k \leq \beta/4$ with $\beta > 0$.

By Lemma 5.1, 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,

$$\underline{x} := \lim_{t \to \infty} x_m(t), \quad \overline{x} := \lim_{t \to \infty} x_M(t) \tag{5.13}$$

For the next developments, we strengthen Lemma 5.1 by showing that there exist normal nodes that settle on the minimum and maximum values in a finite time.

Lemma 5.2. *Consider the network system (5.1)-(5.8), and let Assumptions 5.1 and 5.2 hold. Then, there exist at least two indices $r, s \in \mathbb{N}$ and a finite time $T' \in \mathbb{R}_{\geq 0}$ such that $x_r(t) = \underline{x}$ and $x_s(t) = \overline{x}$ for all $t \geq T'$. In addition, $\min_{i \in \mathbb{N}} x_i(t) \geq \underline{x}$ and $\max_{i \in \mathbb{N}} x_i(t) \leq \overline{x}$ for all $t \geq T'$.*

Proof. We prove the statement only for $\underline{x}$ as the proof for $\overline{x}$ 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 $\underline{\Delta} := \min_{i \in \mathbb{N}} \underline{\Delta}_i$ and pick $\delta = \underline{\Delta}/3$. Consider any $i \in \mathbb{N}$ and any update time t^i_k for node i such that $t^i_k \geq T_\delta$. Condition $t^i_k \geq T_\delta$ is well defined for any T_δ since by Lemma 5.1 normal nodes always remain in the convex hull containing their initial values so that Δ^i_k is bounded from above.

We claim that, for any $i \in \mathbb{N}$ and any $t_k^i \geq T_\delta$,

$$|x_i(t_k^i) - \underline{x}| \geq \delta \;\Rightarrow\; |x_i(t) - \underline{x}| \geq \delta \quad \forall\, t \geq t_k^i \tag{5.14}$$

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 (5.14) 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 $j \in \mathbb{N}$. 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,

$$\begin{aligned} \mathrm{ave}_i(t_k^i) &= \sum_{j \in \mathcal{D}_i(t_k^i)} (z_j(t_k^i) - x_i(t_k^i)) \\ &> \sum_{j \in \mathcal{D}_i(t_k^i)} (\underline{x} - \delta - x_i(t_k^i)) \\ &> -3\delta |\mathcal{D}_i(t_k^i)| \\ &> -\varepsilon \end{aligned} \tag{5.15}$$

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 $j \in \mathbb{N}$. Thus, nodes with an output value less than or equal to $\underline{x} - \delta$ are misbehaving, and they are discarded in view of Assumption 5.1 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 $\mathrm{ave}_i(t_k^i) > -\varepsilon$ 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 $\mathrm{ave}_i(t_k^i) \leq -\varepsilon$. Hence,

$$\begin{aligned} \Delta_k^i &\leq \frac{1}{4d^i} \sum_{j \in \mathcal{D}_i(t_k^i)} (x_i(t_k^i) - z_j(t_k^i)) \\ &< \frac{1}{4d^i} \sum_{j \in \mathcal{D}_i(t_k^i)} (x_i(t_k^i) - \underline{x} + \delta) \\ &\leq \frac{1}{4}(x_i(t_k^i) - \underline{x} + \delta) \end{aligned} \tag{5.16}$$

The second inequality follows because $j \in \mathcal{D}_i(t_k^i)$ only if $z_j(t_k^i) > \underline{x} - \delta$ according with the previous arguments. 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

$$x_i(t) \geq x_i(t_k^i) - \Delta_k^i \geq \underline{x} + \frac{5}{4}\delta \tag{5.17}$$

for all $t \in T_k^i$, where the last inequality follows from (5.16) 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 $i \in \mathbb{N}$, 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 $x_i(\cdot)$, $i \in \mathbb{N}$, either persistently remains inside W or persistently remains outside W. Moreover, there exists at least one index $i \in \mathbb{N}$ for which $x_i(\cdot)$ persistently remains inside W since, by definition, $\underline{x} \in W$ is the limiting value of $x_m(\cdot)$.

Every $x_i(\cdot)$, $i \in \mathbb{N}$, that persistently remains outside W from T'' onwards satisfies $x_i(t) \geq \underline{x} + \delta$ for all $t \geq T''$. Consider next any $x_i(\cdot)$, $i \in \mathbb{N}$, that persistently remains inside W from T'' onwards. 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 $T' := T'' + \varepsilon/4$. This is because, 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 $x_i(t_k^i) \notin W$ according to the previous arguments. Hence, every $x_i(\cdot)$, $i \in \mathbb{N}$, that persistently remains inside W from T'' onwards satisfies $x_i(t) = x_i(T')$ for all $t \geq T'$. Thus $\min_{i \in \mathbb{N}} x_i(t) \geq \underline{x}$ for all $t \geq T'$ and $x_r(T') = \underline{x}$ for some $r \in \mathbb{N}$ since $\underline{x}$ is the limiting value of $x_m(\cdot)$.

5.3 GENERIC MISBEHAVIOR

By Lemma 5.2, there exist at least two indices $r, s \in \mathbb{N}$ and a finite time T' such that $x_r(t) = \underline{x}$ and $x_s(t) = \overline{x}$ for all $t \geq T'$. We now show that under Assumption 5.3 $\overline{x} - \underline{x}$ is upper bounded by 3ε.

Proof of Theorem 5.1. The property that normal nodes always remain inside the convex hull containing their initial values has been shown in Lemma 5.1. Thus, we focus on the second part of the statement.

Let T' be as in Lemma 5.2, and denote by r and s any two indices belonging to $\mathbb{N}$ such that $x_r(t) = \underline{x}$ and $x_s(t) = \overline{x}$ 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 $\mathrm{ave}_r(t_k^r) < \varepsilon$. 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 index $j \in \mathcal{D}_r(t_k^r)$ such that $z_j(t_k^r) - x_r(t_k^r) < 0$. However, this is not possible. In fact, in view of Lemma 5.2, $z_j(t_k^r) = x_j(t_k^r) \geq \underline{x}$ for all $j \in \mathbb{N}$ 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 5.1 and by construction of the control logic. Since every $i \in \mathbb{N}$ satisfies $z_i(\cdot) \equiv x_i(\cdot)$ we have $x_i(t_k^r) - \underline{x} < \varepsilon$ for all $i \in \mathcal{D}_r(t_k^r) \cap \mathbb{N}$.

The claim thus trivially follows if $s \in \mathcal{D}_r(t_k^r)$. Suppose $s \notin \mathcal{D}_r(t_k^r)$. Nodes r and s have at least $3F+1$ neighbors in common by virtue of Assumption 5.3, so that, because of Assumption 5.1, they have at least $2F+1$ neighbors in common belonging to $\mathbb{N}$. 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 because none of these nodes can take on a value larger than $\overline{x}$ from T' onwards in view of Lemma 5.2. Following the same reasoning as before, at least one of these nodes, say node i, must satisfy $x_i(t_k^s) > \overline{x} - \varepsilon$ otherwise one would have $\mathrm{ave}_s(t_k^s) \leq -\varepsilon$. Hence,

$$\begin{cases} x_i(t_k^r) < \underline{x} + \varepsilon \\ x_i(t_k^s) > \overline{x} - \varepsilon \\ x_i(t_k^s) \leq x_i(t_k^r) + \dfrac{\varepsilon}{4} \end{cases} \tag{5.18}$$

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

5.4 DATA ACQUISITION OR TIMING MISBEHAVIOR

Since we are dealing with data acquisition or timing misbehavior, it holds that $z_i(\cdot) \equiv x_i(\cdot)$ for every $i \in \mathcal{I}$. We will therefore only use x_i throughout this section. In order to prove Theorem 5.2, we avail ourselves of the following intermediate result.

Lemma 5.3. *Consider the network system (5.1)-(5.8), with the misbehaving nodes exhibiting an error in the operation (i) and/or (iv). Suppose that Assumptions 5.1 and 5.2 hold. Let T' be as in Lemma 5.2, and let r and s be any two indices belonging to $\mathbb{N}$ such that $x_r(t) = \underline{x}$ and $x_s(t) = \overline{x}$ for all $t \geq T'$. Then, $|\operatorname{ave}_r(t)| < 3\varepsilon/2$ and $|\operatorname{ave}_s(t)| < 3\varepsilon/2$ 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 $t_k^r \geq T'$. As a first step, notice that $\operatorname{ave}_r(t) \geq 0$ for all $t \in T_k^r$ since, in view of Lemma 5.2, $j \in \mathcal{D}_r(t)$ 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 $\operatorname{ave}_r(\cdot)$ over T_k^r.

Following the same notation as in Section 5.1.1, let $\underline{\mathcal{E}}_i(t)$ and $\overline{\mathcal{E}}_i(t)$ 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

$$\begin{cases} \mathcal{A}_r(t) := \mathcal{D}_r(t) \cap \underline{\mathcal{E}}_r(t_k^r) \\ \mathcal{B}_r(t) := \mathcal{D}_r(t) \cap \mathcal{D}_r(t_k^r) \\ \mathcal{C}_r(t) := \mathcal{D}_r(t) \cap \overline{\mathcal{E}}_r(t_k^r) \end{cases} \tag{5.19}$$

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

$$\begin{cases} \underline{\mathcal{C}}_r(t) := \{j \in \mathcal{C}_r(t) : x_j(t) = \underline{x}\} \\ \overline{\mathcal{C}}_r(t) := \{j \in \mathcal{C}_r(t) : x_j(t) > \underline{x}\} \end{cases} \tag{5.20}$$

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 $\overline{\mathcal{C}}_r(t)$. Suppose that there are L elements in this set. Obviously $L \leq F$ since $|\overline{\mathcal{E}}_r(\tau)| \leq F$ for all $\tau \in \mathbb{R}_{\geq 0}$. Now, to each element of $\overline{\mathcal{C}}_r(t)$ there corresponds at least an element belonging to $\mathcal{Z}_r(t) := \overline{\mathcal{E}}_r(t) \cap (\underline{\mathcal{E}}_r(t_k^r) \cup \mathcal{D}_r(t_k^r))$, that is $|\mathcal{Z}_r(t)| \geq L$. In words, if $\overline{\mathcal{C}}_r(t)$ 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, $|\overline{\mathcal{E}}_r(t)| \leq$

$|\overline{\mathcal{E}}_r(t_k^r)| - |\overline{\mathcal{C}}_r(t)| + |\mathcal{Z}_r(t)|$ by construction. Hence, if $|\mathcal{Z}_r(t)| < L$ one would have $|\overline{\mathcal{E}}_r(t)| < |\overline{\mathcal{E}}_r(t_k^r)| \leq F$ along with elements in $\mathcal{D}_r(t)$, those belonging to the set $\overline{\mathcal{C}}_r(t)$, which take on a value larger than $\underline{x}$. However, this is not possible in view of the control logic. Since any element in $\overline{\mathcal{C}}_r(t)$ must take on a value not larger than the value taken on by any element in $\mathcal{Z}_r(t)$, we conclude that

$$\sum_{j \in \mathcal{C}_r(t)} \big(x_j(t) - \underline{x}\big) \leq \sum_{j \in \mathcal{Z}_r(t)} \big(x_j(t) - \underline{x}\big) \tag{5.21}$$

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

$$\begin{cases} \underline{\mathcal{Z}}_r(t) := \overline{\mathcal{E}}_r(t) \cap \underline{\mathcal{E}}_r(t_k^r) \\ \overline{\mathcal{Z}}_r(t) := \overline{\mathcal{E}}_r(t) \cap \mathcal{D}_r(t_k^r) \end{cases} \tag{5.22}$$

Then,

$$\sum_{j \in \mathcal{D}_r(t)} \big(x_j(t) - \underline{x}\big) \leq \sum_{j \in (\mathcal{A}_r(t) \cup \underline{\mathcal{Z}}_r(t))} \big(x_j(t) - \underline{x}\big) + \sum_{j \in (\mathcal{B}_r(t) \cup \overline{\mathcal{Z}}_r(t))} \big(x_j(t) - \underline{x}\big) \tag{5.23}$$

The first sum on the right side of (5.23) yields

$$\begin{aligned} \sum_{j \in (\mathcal{A}_r(t) \cup \underline{\mathcal{Z}}_r(t))} \big(x_j(t) - \underline{x}\big) &\leq \sum_{j \in (\mathcal{A}_r(t) \cup \underline{\mathcal{Z}}_r(t))} \big(x_j(t_k^r) - \underline{x} + t - t_k^r\big) \\ &\leq |\underline{\mathcal{E}}_r(t_k^r)|(t - t_k^r) \end{aligned} \tag{5.24}$$

The first inequality follows since all the nodes, including the misbehaving ones, take controls in $\{-1, 0, 1\}$. The second inequality follows since $(\mathcal{A}_r(t) \cup \underline{\mathcal{Z}}_r(t)) \subseteq \underline{\mathcal{E}}_r(t_k^r)$ and because $j \in \underline{\mathcal{E}}_r(t_k^r)$ only if $x_j(t_k^r) < \underline{x}$. The second sum on the right side of (5.23) yields

$$\begin{aligned} \sum_{j \in (\mathcal{B}_r(t) \cup \overline{\mathcal{Z}}_r(t))} \big(x_j(t) - \underline{x}\big) &\leq \sum_{j \in (\mathcal{B}_r(t) \cup \overline{\mathcal{Z}}_r(t))} \big(x_j(t_k^r) - \underline{x} + t - t_k^r\big) \\ &\leq \varepsilon + |\mathcal{D}_r(t_k^r)|(t - t_k^r) \end{aligned} \tag{5.25}$$

The last inequality follows since $(\mathcal{B}_r(t) \cup \overline{\mathcal{Z}}_r(t)) \subseteq \mathcal{D}_r(t_k^r)$ and since $\sum_{j\in\mathcal{S}} \left(x_j(t_k^r) - \underline{x}\right) < \varepsilon$ for every $\mathcal{S} \subseteq \mathcal{D}_r(t_k^r)$. In fact, $\sum_{j\in\mathcal{D}_r(t_k^r)} \left(x_j(t_k^r) - \underline{x}\right) < \varepsilon$ since r stays constant from T' on. Thus, in order for $\sum_{j\in\mathcal{S}} \left(x_j(t_k^r) - \underline{x}\right) \geq \varepsilon$ there should exist at least one node $j \in \mathcal{D}_r(t_k^r)\backslash\mathcal{S}$ 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 $x_j(t_k^r) \geq \underline{x}$ otherwise it is discarded in view of Assumption 5.1 and by construction of the control logic.

Overall, we get

$$\begin{aligned}\sum_{j\in\mathcal{D}_r(t)} \left(x_j(t) - \underline{x}\right) &\leq \varepsilon + (|\underline{\mathcal{E}}_r(t_k^r)| + |\mathcal{D}_r(t_k^r)|)(t - t_k^r) \\ &< \frac{3}{2}\varepsilon \end{aligned} \tag{5.26}$$

for all $t \in T_k^r$ since $|\underline{\mathcal{E}}_r(t_k^r)| + |\mathcal{D}_r(t_k^r)| \leq d_r$ 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 $|\operatorname{ave}_r(\cdot)| < 3\varepsilon/2$ 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 $|\operatorname{ave}_r(t)| < 3\varepsilon/2$ for all $t \geq T$.

We note that Lemma 5.3 strongly relies on the fact that there is no control or transmission misbehavior. In fact, in either case, neither (5.24) nor (5.25) are valid.

We finally proceed with the proof of Theorem 5.2.

Proof of Theorem 5.2. Let T be as in Lemma 5.3, and denote by r and s any two indices belonging to $\mathbb{N}$ such that $x_r(t) = \underline{x}$ and $x_s(t) = \overline{x}$ for all $t \geq T$.

Consider any $t \geq T$. We have

$$\operatorname{ave}_s(t) = \sum_{j\in\mathcal{D}_s(t)} \left(x_j(t) - \overline{x}\right) = \sum_{j\in\mathcal{D}_s(t)} \left(x_j(t) - \underline{x}\right) + |\mathcal{D}_s(t)|\left(\underline{x} - \overline{x}\right) \tag{5.27}$$

The sum term satisfies

$$\begin{aligned}\sum_{j\in\mathcal{D}_s(t)} \left(x_j(t) - \underline{x}\right) &= \sum_{j\in(\mathcal{D}_s(t)\backslash\mathcal{D}_r(t))} \left(x_j(t) - \underline{x}\right) + \sum_{j\in(\mathcal{D}_s(t)\cap\mathcal{D}_r(t))} \left(x_j(t) - \underline{x}\right) \\ &< \sum_{j\in(\mathcal{D}_s(t)\backslash\mathcal{D}_r(t))} \left(x_j(t) - \underline{x}\right) + \frac{3}{2}\varepsilon \end{aligned} \tag{5.28}$$

The inequality comes from the fact that $\mathrm{ave}_r(t) < 3\varepsilon/2$ in view of Lemma 5.3, and since $\sum_{j\in\mathcal{S}} \left(x_j(t) - \underline{x}\right) < 3\varepsilon/2$ for every $\mathcal{S} \subseteq \mathcal{D}_r(t)$ (*cf.* the proof of Lemma 5.3). Hence,

$$\mathrm{ave}_s(t) < \sum_{j\in(\mathcal{D}_s(t)\setminus\mathcal{D}_r(t))} \left(x_j(t) - \underline{x}\right) + |\mathcal{D}_s(t)|\,(\underline{x} - \overline{x}) + \frac{3}{2}\varepsilon \tag{5.29}$$

Since s is the node attaining the maximum value among the normal nodes, $j \in \mathcal{D}_s(t)$ only if $x_j(t) \leq \overline{x}$ otherwise it is discarded in view of Assumption 5.1 and by construction of the control logic. Thus, $x_j(t) \leq \overline{x}$ for all $t \geq T$ and all $j \in \mathcal{D}_s(t)$. Hence,

$$\mathrm{ave}_s(t) < \left(|\mathcal{D}_s(t)\setminus\mathcal{D}_r(t)| - |\mathcal{D}_s(t)|\right)(\overline{x} - \underline{x}) + \frac{3}{2}\varepsilon \tag{5.30}$$

As a final step, notice that

$$|\mathcal{D}_s(t)| - |\mathcal{D}_s(t)\setminus\mathcal{D}_r(t)| = |\mathcal{D}_s(t) \cap \mathcal{D}_r(t)| \tag{5.31}$$

Following the same notation as in Section 5.1.1, let $\underline{\mathcal{E}}_i(t)$ and $\overline{\mathcal{E}}_i(t)$ be the set of nodes discarded by $i \in \mathbb{N}$ at time t with associated value smaller than $x_i(t)$ and larger than $x_i(t)$, respectively. For nodes r and s, define

$$\begin{cases} \underline{\mathcal{W}}_r(t) := \underline{\mathcal{E}}_r(t) \cap \mathcal{Q}_s \\ \overline{\mathcal{W}}_r(t) := \overline{\mathcal{E}}_r(t) \cap \mathcal{Q}_s \\ \underline{\mathcal{W}}_s(t) := \underline{\mathcal{E}}_s(t) \cap \mathcal{Q}_r \\ \overline{\mathcal{W}}_s(t) := \overline{\mathcal{E}}_s(t) \cap \mathcal{Q}_r \end{cases} \tag{5.32}$$

Thus, at every $t \in \mathbb{R}_{\geq 0}$, node r discards $|\underline{\mathcal{W}}_r(t)| + |\overline{\mathcal{W}}_r(t)|$ nodes that are also neighbors of s. Similarly, node s discards $|\underline{\mathcal{W}}_s(t)| + |\overline{\mathcal{W}}_s(t)|$ nodes that are also neighbors of r. Moreover,

$$\begin{cases} \underline{\mathcal{W}}_r(t) \subseteq \underline{\mathcal{W}}_s(t) \\ \overline{\mathcal{W}}_s(t) \subseteq \overline{\mathcal{W}}_r(t) \end{cases} \tag{5.33}$$

The first relation follows because r is the node attaining the minimum value among the normal nodes. Thus, all the nodes that belong to $\underline{\mathcal{W}}_r(t)$ take on value less than $\underline{x}$ and hence are necessarily misbehaving. Since these nodes belong to $\mathcal{Q}_s$, they must be discarded also by node s. In fact, at every $t \in \mathbb{R}_{\geq 0}$, node s discards the F smallest value less than $x_s(t)$, and, after T, there cannot be more than F values less than $\underline{x}$ in view of Assumption 5.1 and Lemma 5.2. Hence, these nodes must belong to $\underline{\mathcal{E}_s}(t)$, and thus to $\underline{\mathcal{W}}_s(t)$. The same reasoning applies to the relation $\overline{\mathcal{W}}_s(t) \subseteq \overline{\mathcal{W}}_r(t)$.

Hence, at every $t \in \mathbb{R}_{\geq 0}$, nodes r and s can discard at most $|\underline{\mathcal{W}}_s(t)| + |\overline{\mathcal{W}}_r(t)| \leq 2F$ different common neighbors. Since by Assumption 5.4 nodes r and s have at least $2F+1$ neighbors in common, we have $|\mathcal{D}_s(t) \cap \mathcal{D}_r(t)| \geq 1$. This implies that $\mathrm{ave}_s(t) < -(\overline{x} - \underline{x}) + 3\varepsilon/2$. By combining this inequality with $\mathrm{ave}_s(t) > -3\varepsilon/2$, we finally conclude that $\overline{x} - \underline{x} < 3\varepsilon$.

5.5 A NUMERICAL EXAMPLE

Consider a network system as in (5.1)-(5.8), with $n = 7$ nodes interconnected as in Figure 5.1 and $F = 1$ misbehaving nodes. State and clock initial values are taken randomly within the intervals $[0, 1]$ and $[0, t_{init}]$, respectively, with $t_{init} = 0.15sec$. The desired accuracy level for consensus is selected as $\varepsilon = 0.01$ and we set $\underline{\Delta}_i = \varepsilon/(4d^i)$ for every node. We note that the graph satisfies Assumption 5.3, which is sufficient to guarantee resilience against generic misbehavior (Theorem 5.1).

We mainly consider the case of control and output misbehavior, which are the most critical errors for consensus (*cf.* Section 5.1.2) and depict tangible variation in state and output evolution. Specifically, we assume that the misbehaving node $i \in \mathcal{M}$ applies the control input $u_i(t) = 10 \sin(10\,\pi t)$ and $u_i(t) = 0.2$ for all $t \in \mathbb{R}_{\geq 0}$ instead of (5.5). Figure 5.2 and 5.3 illustrates the network state evolution with the proposed resilient consensus protocol. In agreement with the conclusions of Theorem 5.1, one sees that the normal nodes remain in the convex hull containing their initial values and reach an approximate agreement disregarding the behavior of the misbehaving node.

In order to further substantiate the performance of the proposed resilient coordination protocol, we consider other type of attack strategies. For example in Figure 5.4, 5.5, and 5.6 we consider output misbehavior where the evolution of the output of the misbehaving node $i \in \mathcal{M}$ follows an arbitrary trajectory according $z_i(t) = 0.05 \sin(10\pi t + x_i(0)$, $z_i(t) = 0.5t + x_i(0)$, and $z_i(t) = 0.1 + x_i(0)$, respectively. While we observe the employed resilient protocol ensures network nodes reach consensus.

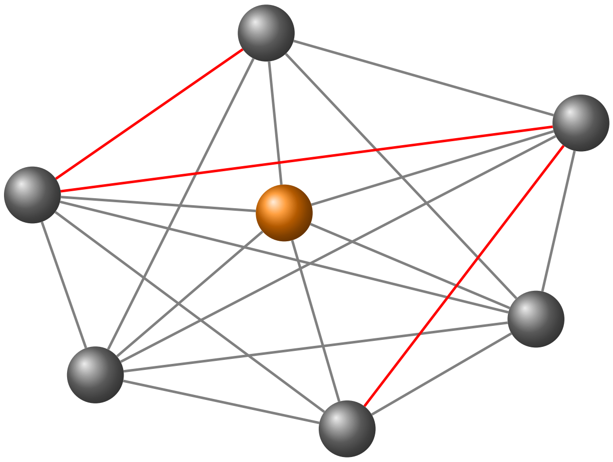

Figure 5.1: Network system considered in the numerical example. Normal nodes are depicted in gray, while the misbehaving node is depicted in orange. The graph satisfies Assumption 5.3 and is thus robust against generic misbehavior (Theorem 5.1). The removal of the red edges leads to a graph that satisfies Assumption 5.4, which is robust against data acquisition or timing misbehavior (Theorem 5.2).

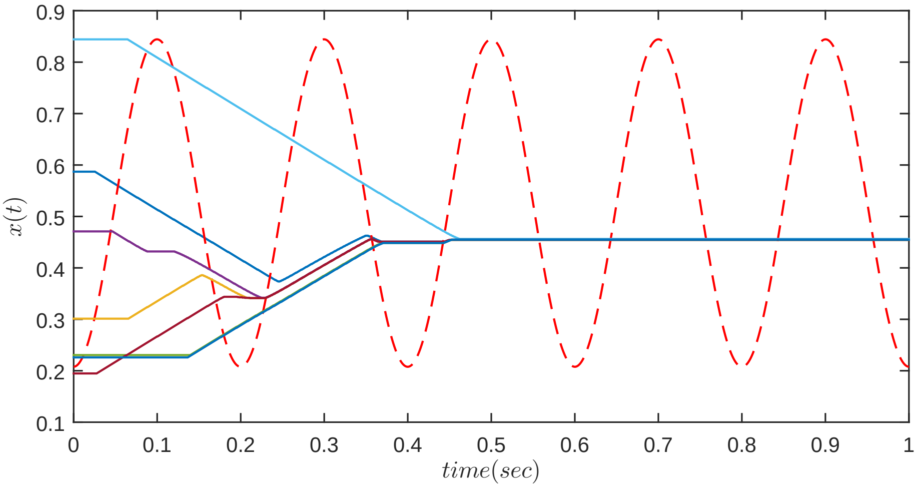

Figure 5.2: Network state evolution with the resilient consensus protocol under control misbehavior $u_i(t) = 10\sin(10\,\pi t), i \in \mathcal{M}$. The evolution of the misbehaving node's state is depicted in red dashed line.

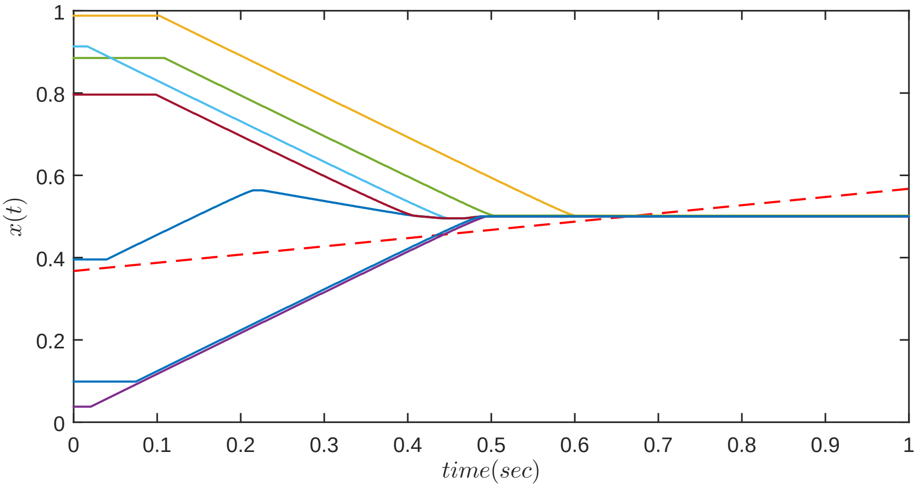

Figure 5.3: Network state evolution with the resilient consensus protocol under control misbehavior, $u_i(t) = 0.2, i \in \mathcal{M}$. The evolution of the misbehaving node's state is depicted in red dashed line.

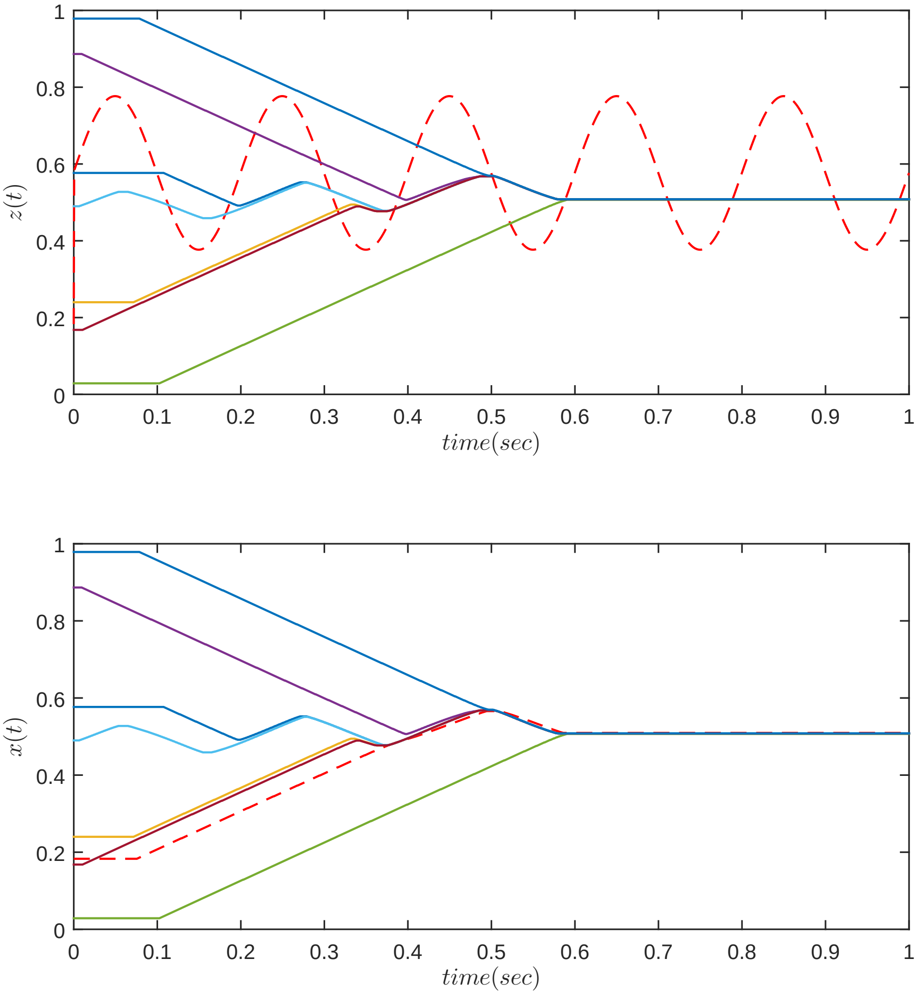

Figure 5.4: Network state $x(t)$ and output $z(t)$ evolution under output misbehavior $z_i(t) = 0.2\sin(10\pi t) + x_i(0)$, $i \in \mathcal{M}$. The misbehaving node trajectories are depicted in red dashed line.

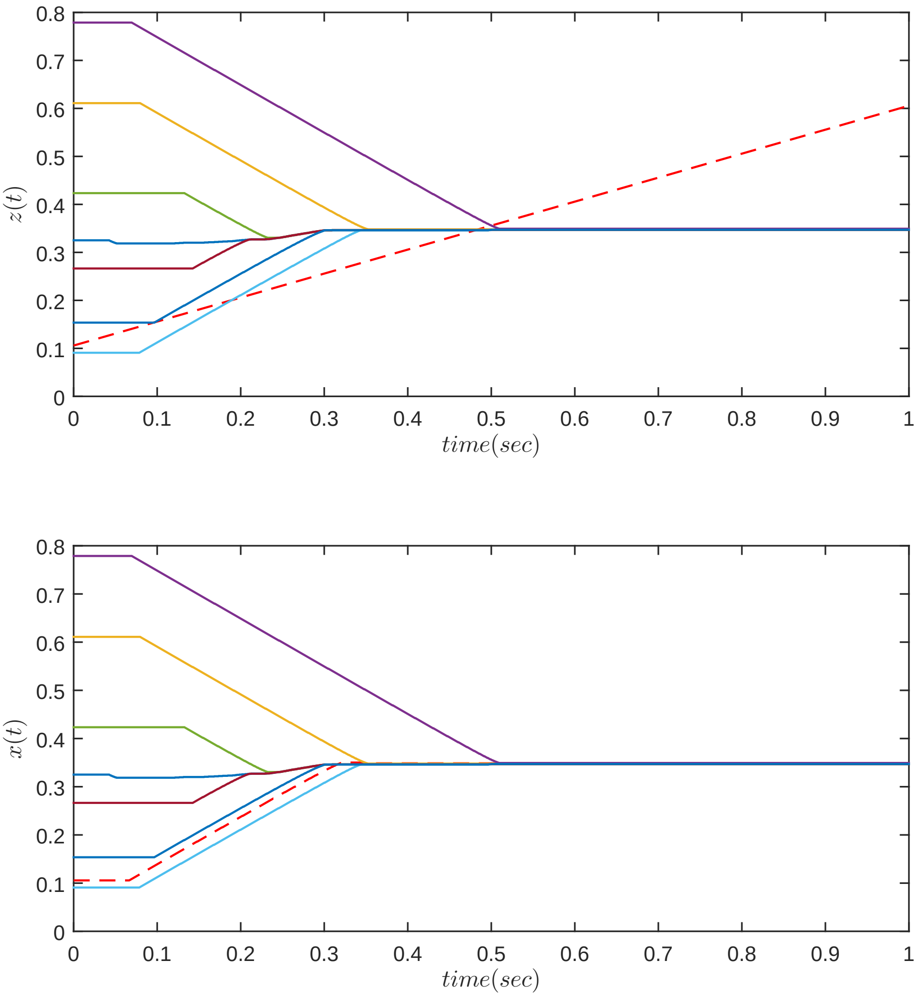

Figure 5.5: Network state $x(t)$ and output $z(t)$ evolution under output misbehavior $z_i(t) = 0.5\,t + x_i(0)$, $i \in \mathcal{M}$. The misbehaving node trajectories are depicted in red dashed line.

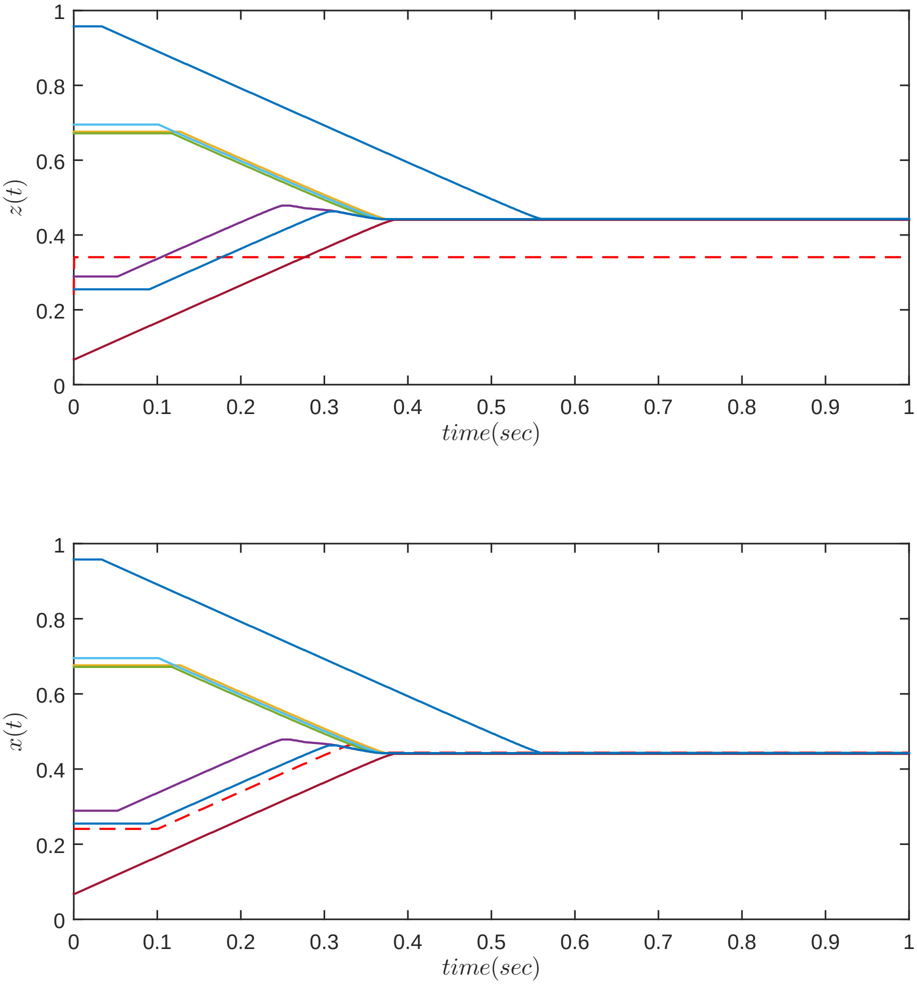

Figure 5.6: Network state $x(t)$ and output $z(t)$ evolution under output misbehavior $z_i(t) = 0.1 + x_i(0)$, $i \in \mathcal{M}$. The misbehaving node trajectories are depicted in red dashed line.

6 Misbehavior-Resilient Asymptotic Coordination in Self-triggered Networks

ABSTRACT

By reasoning on approximate consensus, the connectivity conditions in chapter 5 are more conservative than those found in the literature on resilience coordination under synchronous clocks LeBlanc et al. (2013). In particular. The objective of this chapter is to relax the network connectivity requirement of chapter 5 by reasoning on asymptotic consensus. The considered approach is inspired by the asymptotic coordination protocol De Persis and Frasca (2013), where exact consensus is achieved at the expense of slowing down the convergence speed. The idea is that exact consensus helps to reduce some constraints on the network connectivity. Although the formal analysis of this new protocol is not yet complete, it is conjectured that with this modification we can ensure resilience under the same (r, s)-robustness hypothesis of LeBlanc et al. (2013).

Published as:

6.1 SYSTEM DEFINITION

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, with $n := |\mathcal{I}|$, while $\mathcal{E} \subseteq \mathcal{I} \times \mathcal{I}$ is the set of edges. We let $\mathcal{Q}_i$ denote the set of neighbors of $i \in \mathcal{I}$, and by d_i the cardinality of $\mathcal{Q}_i$, that is $d_i := |\mathcal{Q}_i|$. 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

$$\begin{cases} \dot{x}_i(t) = \gamma(t)\, u_i(t) \\ z_i(t) = f_i(x_i(t)) \end{cases} \qquad t \in \mathbb{R}_{\geq 0} \tag{6.1}$$

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; $\gamma(t) = a/1 + t,\ \forall a \in \mathbb{R}_{\geq 0}$ is a non-increasing function; $z_i \in \mathbb{R}$ is the output, where $f_i : \mathbb{R} \to \mathbb{R}$ 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 *asymptotic* consensus despite the presence of misbehaving nodes. The class of misbehavior in this chapter is similar to chapter 5. 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.

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

- Let $\varepsilon(t) = b/1 + t,\ \forall b \in \mathbb{R}_{\geq 0}$ be a non-increasing function, such that $\lim_{t \to \infty} \varepsilon(t) = 0$.
- A parameter $F \in \mathbb{N}$, which determines the maximum number of misbehaving nodes that the network is expected to encounter.
- A sequence $\{t_k^i\}_{k \in \mathbb{N}}$ of time instants at which node i requests data from its neighbors, where $t_0^i \in [0, t_{init}]$ defines the first time instant at which node i becomes active and $t_{init} \in \mathbb{R}_{\geq 0}$ 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 $i \in I$ 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.

6.1.1 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. We now focus on the generic k-th round of operations for node $i \in \mathcal{N}$. This consists of four main operations: *(i) data acquisition*; *(ii) data transmission*; *(iii) control logic*; *(iv) timing*. The operations *(i)*, *(ii)*, and *(iii)* are similar to chapter 5. The update time operation *(iv)*, however, should be adjusted to compensate for slowing the system velocity by $\gamma(t)$ and avoids arbitrarily fast update rate. Error or fault in any of the mentioned operations is considered as misbehavior.

(iv) Timing. For $i \in \mathcal{N}$, the next round of operations is scheduled at time $t^i_{k+1} = t^i_k + \Delta^i_k$ where

$$\Delta^i_k = \frac{1}{4d^i\gamma(t^i_k)} \max\{\varepsilon(t^i_k), |\,\mathrm{ave}_i(t^i_k)|\} \tag{6.2}$$

with $\underline{\Delta}_i \in \mathbb{R}_{>0}$ such that $\underline{\Delta}_i := \min_k \Delta^i_k \leq c/4d_{\max}$ and $c \in \mathbb{R}_{>0}$ satisfies

$$c \leq \frac{\varepsilon(t)}{\gamma(t)}, \qquad \forall\, t \geq 0 \tag{6.3}$$

Operations can be then periodic as well as aperiodic. Parameter $\varepsilon(t)$ asymptotically converges to zero, parameter $\gamma(t)$ in (6.1) is introduced to avoids arbitrarily fast sampling (Zeno behavior) by slowing down the update rate of system (6.2) and the system velocity (6.1). To fulfill this purpose, therefore, the non-increasing functions $\varepsilon(t)$ and $\gamma(t)$ should enjoy a comparable speed of convergence to zero that satisfies (6.3). A timing error means that (6.2) is not satisfied for some $k \in \mathbb{N}$.

6.1.2 ASSUMPTIONS AND DEFINITIONS

Assumption 6.1. *The set $\mathcal{M}$ of misbehaving nodes does not change over time and each normal node i can have at most F misbehaving node among its neighbors, i.e. $|\mathcal{Q}_i \cap \mathcal{M}| \leq F$.*

Assumption 6.2. *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 $k \in \mathbb{N}$, $i \in \mathcal{M}$, and for some $\underline{\Delta}_i \in \mathbb{R}_{>0}$.*

Definition 6.1 ((r, s)-robust graph)**.** For $r, s \in \mathcal{N}$, the graph for all pairs of disjoint nonempty subsets of nodes $S_1, S_2 \subset \mathcal{I}$, satisfies at least one of the following conditions

i All nodes in S_1 have at least r neighbors outside S_1.

ii All nodes in S_2 have at least r neighbors outside S_2.

iii There are at least s nodes in $S_1 \cup S_2$ that each have at least r neighbors outside their respective sets.

The Assumption 6.2 ensures the existence of the solutions for all the nodes and for all time, that variables and functions are well defined. Furthermore, it entails no upper bound on $\Delta_k^i, \forall i \in \mathcal{M}$. This is in order to capture the event that a misbehaving node never collects data from its neighbors and applies an open-loop control.

Definition 6.1 deals with the graph connectivity properties and ensure that the normal nodes enjoy sufficient "genuine" information for taking control decisions LeBlanc et al. (2013). These assumptions should be interpreted as design conditions when the graph topology can be assigned.

In the next section we sate the main results of the paper.

6.2 MAIN RESULT

Before representing the main result of this chapter. Let the maximum and minimum trajectories be defined as

$$x_m(t) := \min_{i \in \mathcal{N}} x_i(t), \qquad x_M(t) := \max_{i \in \mathcal{N}} x_i(t) \tag{6.4}$$

where $t \in \mathbb{R}_{\geq 0}$.

In order to argue that all normal nodes remain in the convex hull containing their initial values first we have to show $x_M(t)$ and $x_m(t)$ are monotonically non-increasing and non-decreasing, respectively. This argument is given in Lemma 6.1.

Lemma 6.1. *Consider the network system (6.1)-(6.2), and let Assumptions 6.1 and 6.2 hold. Then, $x_m(\cdot)$ and $x_M(\cdot)$ are monotonically non-decreasing and non-increasing, respectively.*

Proof of Lemma 6.1. 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 an index $i \in \mathcal{N}$ such that

$$\begin{cases} x_i(\tau) \le x_j(\tau) \quad \forall j \in \mathcal{N} \\ u_i(\tau) < 0 \end{cases} \tag{6.5}$$

Clearly, there could be multiple nodes achieving (6.5) at time τ. In this case, i is any of such nodes. Notice that $\tau \ge t_0^i$ 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 $\mathrm{ave}_i(t_k^i) \le -\varepsilon < 0$. However, this is not possible. In fact, any normal node j satisfies $z_j(t_k^i) = x_j(t_k^i) \ge x_i(t_k^i)$ because i is the node of minimum at $\tau = t_k^i$. Hence, $z_j(t_k^i) < x_i(t_k^i)$ only if j is misbehaving. Since misbehaving nodes are not more than F by Assumption 6.1, if a misbehaving node j gives $z_j(t_k^i) < x_i(t_k^i)$ 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 (6.5), there must exist a node $s \in \mathcal{N}$ such that

$$\begin{cases} x_s(t_k^i) \le x_j(t_k^i) \quad \forall j \in \mathcal{N} \\ x_s(t_k^i) < x_i(t_k^i) \\ x_i(\tau) \le x_j(\tau) \quad \forall j \in \mathcal{N} \\ u_i(\tau) < 0 \end{cases} \tag{6.6}$$

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 $u_i(t_k^i) \ge 0$ 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 $\tau - t^i_k \geq \beta/2\gamma(t^i_k)$. However,

$$\begin{aligned} \Delta^i_k(t^i_k) &\leq \frac{1}{4d^i\gamma(t^i_k)} \sum_{j\in\mathcal{D}_i(t^i_k)} (x_i(t^i_k) - z_j(t^i_k)) \\ &\leq \frac{1}{4d^i\gamma(t^i_k)} \sum_{j\in\mathcal{D}_i(t^i_k)} (x_i(t^i_k) - x_s(t^i_k)) \end{aligned} \tag{6.7}$$

The first equality follows from the fact that $u_i(t^i_k) < 0$ requires $\mathrm{ave}_i(t^i_k) \leq -\varepsilon(t^i_k)$ so that $\Delta^i_k \leq |\,\mathrm{ave}_i(t^i_k)|/(4d^i\gamma(t^i_k))$. On the other hand, the second inequality follows since $z_j(t^i_k) < x_s(t^i_k)$ only if j is misbehaving, in which case it is discarded by node i in view of Assumption 6.1 and by the control logic. Since $|\mathcal{D}_i(t)| \leq d^i$ for all $t \in \mathbb{R}_{\geq 0}$ then $\Delta^i_k \leq \beta/4\gamma(t^i_k)$. This leads to a contradiction since it implies

$$\frac{\beta}{2\gamma(t^i_k)} \leq \tau - t^i_k < \Delta^i_k \leq \frac{\beta}{4\gamma(t^i_k)}$$

with $\beta > 0$.

This Lemma implies that $x_M(t)$ and $x_m(t)$ admit a finite limit

$$\underline{x} := \lim_{t\to\infty} x_m(t), \quad \overline{x} := \lim_{t\to\infty} x_M(t) \tag{6.8}$$

We conjecture that $\overline{x} = \underline{x}$ under the hypothesis that the graph is $(F+1, F+1)$-robust, meaning that the network achieves exact consensus. More precisely , we conjecture the following.

Conjecture 6.1. *Consider the network system (6.1)-(6.2), with the misbehaving nodes exhibiting an error in either of the operations (i)-(iv). If Assumptions 6.1 and 6.2 hold true and the graph is $(F+1, F+1)$-robust, then for all $i \in \mathcal{N}$, $x_i(t)$ remains inside the convex hull containing their initial values and*

$$\lim_{t\to\infty} x_i(t) = v, \qquad v \in [\min_i\{x_i(0)\},\ \max_i\{x_i(0)\}]$$

The above conjecture is based on the following considerations. With approximate consensus of chapter 5 nodes can stop updating their values even if exact consensus is not achieved, in which case $\overline{x} = \underline{x}$ can be large (increasing with network size). As discussed in chapter 5, Assumption 5.3 and 5.4 become instrumental to ensure that the nodes attaining the maximum $\overline{x}$ and minimum $\underline{x}$ values share enough genuine (non-misbehaving) information so that $\overline{x} - \underline{x}$ can be kept small. By using a protocol that searches for exact consensus, nodes can stop updating their values only when exact consensus is achieved. Since the nodes of maximum and minimum take on a limiting value, in order to show that $\overline{x} = \underline{x}$ one hast to rule out the situation where some of the network nodes take on value within $[\underline{x}, \overline{x}]$ and continue to move, which in principle would allow $\overline{x} - \underline{x}$ to be strictly grater than zero. We conjecture that this situation can not happen if the graph is $(F+1, F+1)$-robust since this property guarantees that asymptotically at least one of the two nodes taking on maximum and minimum values have at least $F+1$ neighbors, thus at least one genuine (non-misbehaving) node. This implies that such neighbor must necessarily take on the same maximum/minimum constant value. In turn, by applying iteratively the same argument this ensures that $\overline{x} = \underline{x}$. Unfortunately, the above argument holds only when $\overline{x}$ and $\underline{x}$ are exactly attained, which is true only asymptotically. This introduces some technical subtleties which need to be worked out in order to make the above argument rigorous. In sequel, this idea is demonstrated via numerical example. Extensive simulation results indicate that most likely this conjecture is true.

As a final point we mention that while this modified protocol can provide a way to relax the hypothesis on the network connectivity, it remains interesting to see if one can relax the hypothesis in the network connectivity also with respect to the protocol of section 5 which has the definite advantage to ensure finite-time convergence.

6.3 A NUMERICAL EXAMPLE

Consider a network system as in (6.1)-(6.2), with $n = 7$ and $d_{\max} = 5$ nodes interconnected as in Fig. 6.1 and $F = 1$ misbehaving nodes. State and clock initial values are taken randomly within the intervals $[0, 1]$ and $[0, t_{init}]$, respectively, with $t_{init} = 0.5 sec$. As far as simulation is concerned, the desired functions $\varepsilon(t) = 0.05/(1+t)$ and $\gamma(t) = 0.25/(1+t)$ are assumed. This sets $\underline{\Delta} = 0.025$ for every node with $c = 0.2$. We note that the graph satisfies $(2, 2)$-robust property as in Definition 6.1.

We mainly consider the case of control and output misbehavior, which are the most critical errors for consensus and depict tangible variation in state and

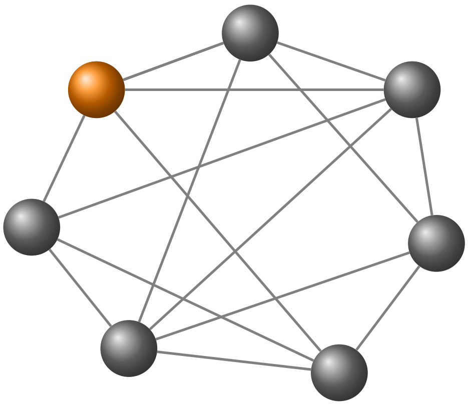

Figure 6.1: Network system considered in the numerical example. Normal nodes are depicted in grey, while the misbehaving node is depicted in orange. The graph satisfies $(2,2)$-robust property as in Definition 6.1.

output evolution. Specifically, we assume that the misbehaving node $i \in \mathcal{M}$ applies the control input $u_i(t) = 10\sin(10\,\pi t)$ and $u_i(t) = 0.05$ for all $t \in \mathbb{R}_{\geq 0}$ instead of (5.5). Figure 6.2 and 6.3 illustrates the network state evolution with the proposed resilient consensus protocol. In agreement with the conclusions of Theorem 6.1, one sees that the normal nodes remain in the convex hull containing their initial values and reach an approximate agreement disregarding the behavior of the misbehaving node.

In order to further substantiate the performance of the proposed resilient coordination protocol, we consider other type of misbehavior. For example in Figure 6.4, 6.5, and 6.6 we consider output misbehavior where the evolution of the output of the misbehaving node $i \in \mathcal{M}$ follows an arbitrary trajectory according $z_i(t) = 0.3\sin(\pi t + x_i(0)$, $z_i(t) = 0.06\,t + x_i(0)$, and $z_i(t) = 0.1 + x_i(0)$, respectively.

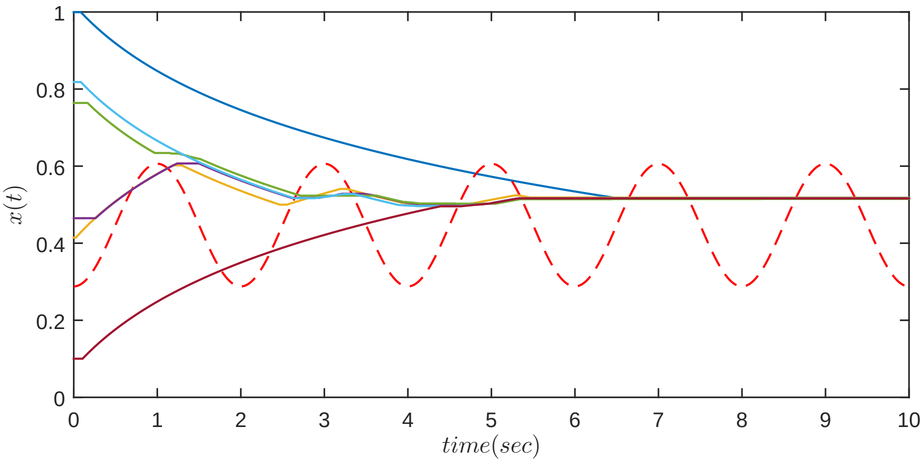

Figure 6.2: Network state evolution with the resilient consensus protocol under control misbehavior $u_i(t) = 0.5\sin(\pi t), i \in \mathcal{M}$. The evolution of the misbehaving node's state is depicted in red dashed line.

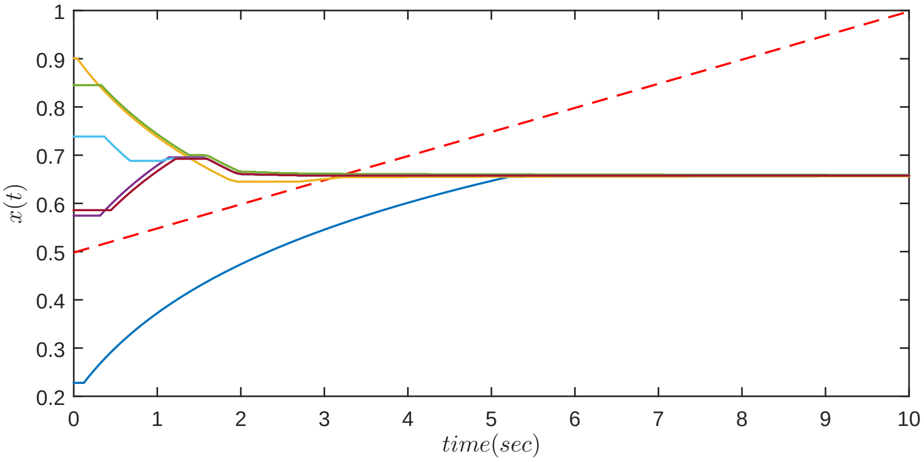

Figure 6.3: Network state evolution with the resilient consensus protocol under control misbehavior, $u_i(t) = 0.05, i \in \mathcal{M}$. The evolution of the misbehaving node's state is depicted in red dashed line.

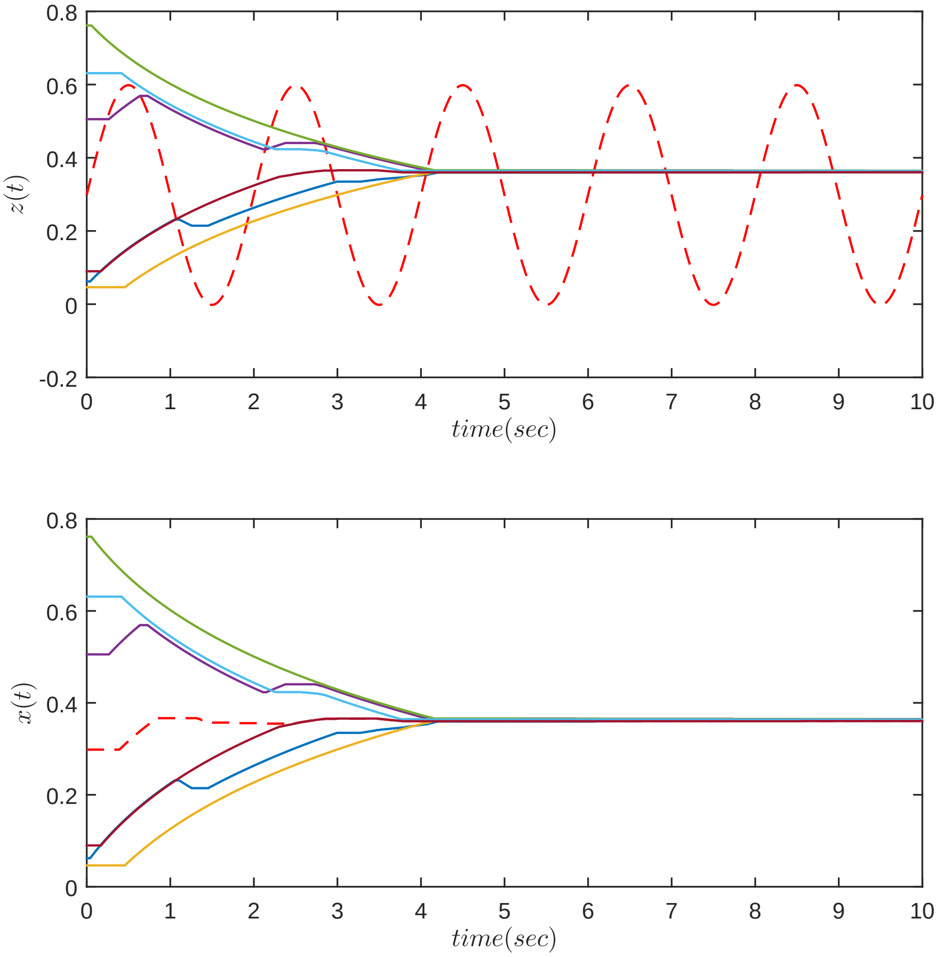

Figure 6.4: Network state $x(t)$ and output $z(t)$ evolution under output misbehavior $z_i(t) = 0.3\sin(\pi t) + x_i(0)$, $i \in \mathcal{M}$. The misbehaving node trajectories are depicted in red dashed line.

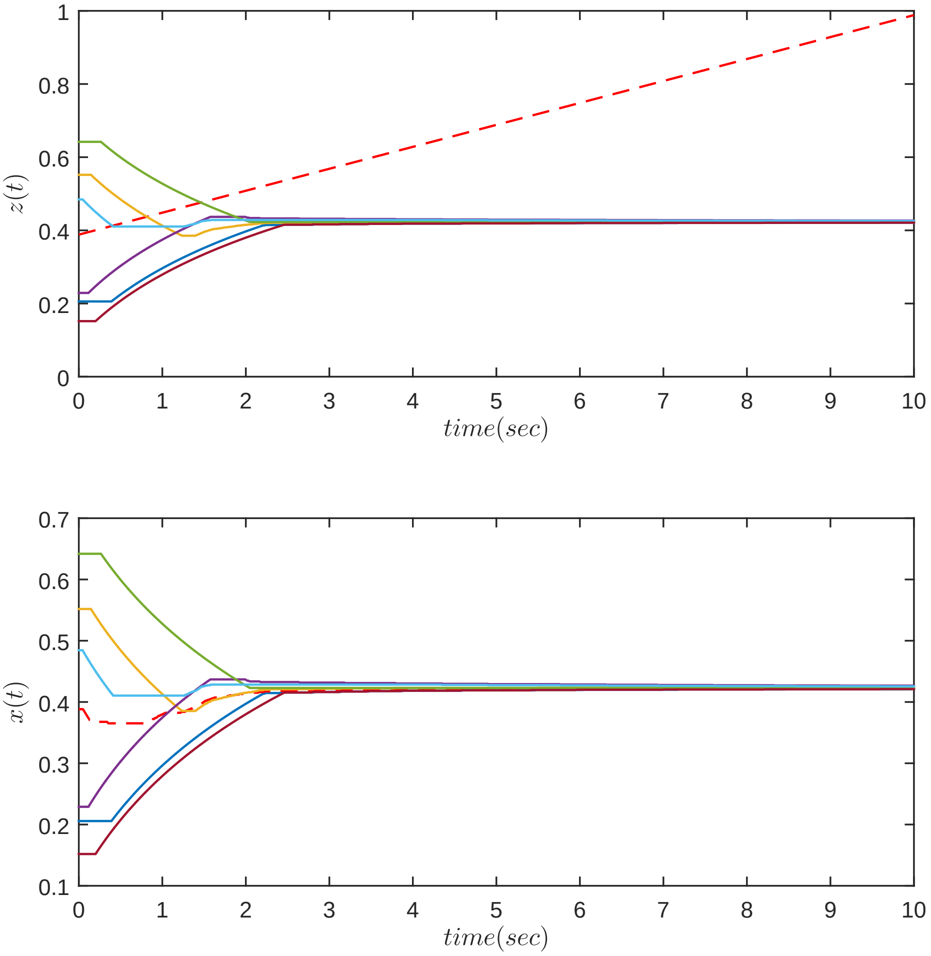

Figure 6.5: Network state $x(t)$ and output $z(t)$ evolution under output misbehavior $z_i(t) = 0.06\,t + x_i(0)$, $i \in \mathcal{M}$. The misbehaving node trajectories are depicted in red dashed line.

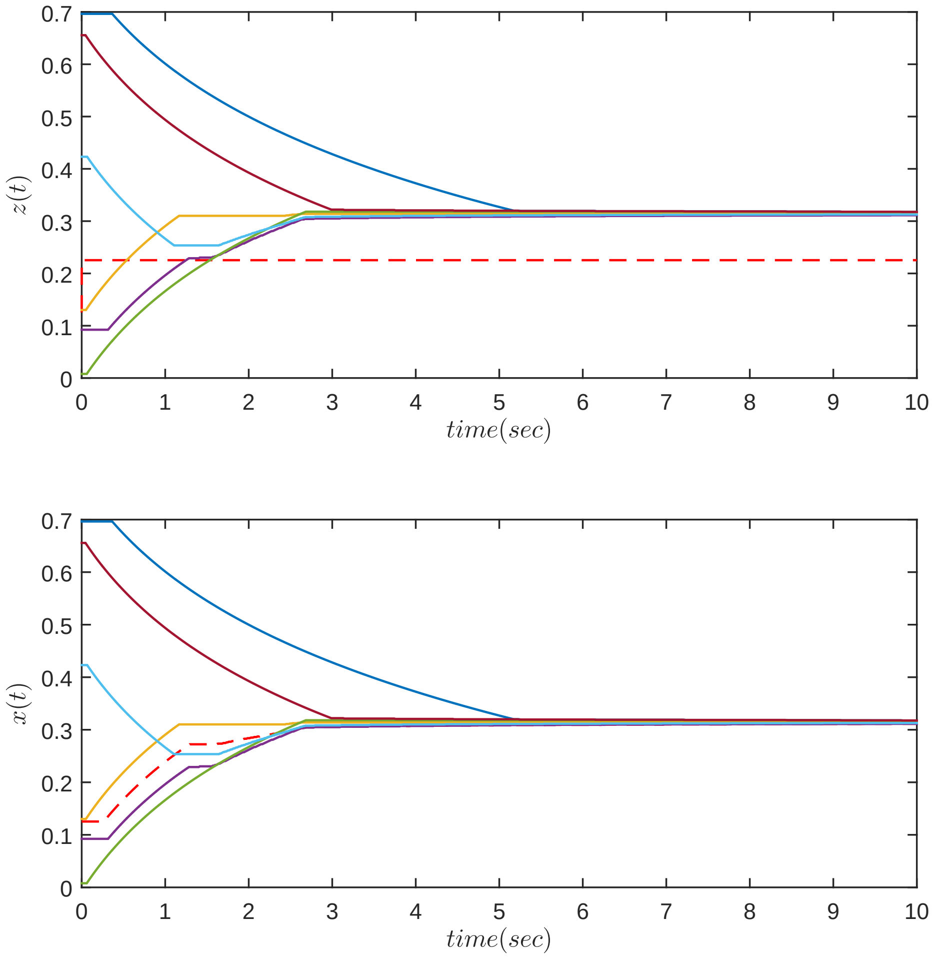

Figure 6.6: Network state $x(t)$ and output $z(t)$ evolution under output misbehavior $z_i(t) = 0.1 + x_i(0)$, $i \in \mathcal{M}$. The misbehaving node trajectories are depicted in red dashed line.

7 Conclusions

In this thesis, we developed self-triggered coordination protocols that are resilient against communication failure and node misbehavior of both genuine and malicious nature. These scenarios are representatives of breach in data availability and integrity, respectively, which are the dominant threats to cyber-physical systems.

In part I, we investigated self-triggered coordination for distributed network systems in the presence of Denial-of-Service at the communication links, of both genuine and malicious nature. We considered a framework in chapter 2 in which DoS affects the whole network links simultaneously, which is representative for networks operating at infrastructure mode. A generalized version of this framework is considered in chapter 3 and 4 in which DoS can affect each of the network links independently, which is representative for networks operating in peer-to-peer mode. By introducing a notion of Persistency-of-Communication (PoC), we provided an explicit characterization of DoS frequency and duration under which coordination of single integrator dynamics (chapter 2 and 3) and synchronization of higher order dynamics (chapter 4) can be preserved by suitably designing time-varying control and communication policies. An explicit characterization of the effects of DoS on the consensus and synchronization time has also been provided. We compared the notion of PoC with classic average connectivity conditions that are found in pure continuous-time consensus networks. The analysis reveals that PoC naturally extends such classic conditions to a digital networked setting by requiring graph connectivity over periods of time that are consistent with the constraints imposed by the communication medium.

In part II, we investigated 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. The results in chapter 5 indicate that handling misbehaving units can be possible also in network applications involving asynchronous and aperiodic transmissions, as occurs with event-triggered and self-triggered network systems. In chapter 6 the connectivity condition required to achieve approximate consensus in chapter 5 is relaxed via a different coordination protocol, following the similar line of reasoning in LeBlanc et al. (2013). A rigorous treatment of convergence for this protocol is still under development.

7.1 FUTURE RESEARCH

High network connectivity helps to render the network more robust against DoS and misbehavior, while low network connectivity helps to save communication resources. The former and latter are concerned with robustness and communication cost, respectively. Optimizing the trade off between robustness and communication cost is an interesting topic for future research. A detail elaboration on possible future works are provided for part I and II, separately.

7.1.1 PART I

The presented results lend themselves to many extensions. An interesting investigation pertains the analysis of coordination and synchronization schemes in the presence of both DoS and deceptive attacks. In this part, failures induced by DoS do not follow a given class of probability distributions. It can be interesting to consider a probabilistic approach in case the attacker does also want to remain undetected; see for instance Zhang et al. (2015); Bai et al. (2015). This is because for example packet drops following a Bernoulli distribution or alike might be more difficult to detect with classic detectors, as they might resemble genuine packet drops. Investigating this issue in the present context represents an interesting research line.

Finally, it is of interest to look for control laws other than the one considered in this thesis. For instance, one can think of embedding the nodes with prediction capabilities so as to estimate the behavior of the neighboring nodes and set the control action accordingly, possibly in accordance with a given optimality performance criterion. A choice of this type has been considered in Feng and Tesi (2017), where the control action during DoS is chosen based on predictions of the process future behavior. The analysis in Feng and Tesi (2017), however, is restricted to a classic single-feedback control loop, and it is not immediately clear how such an approach can be extended to a distributed setting like the one considered in this thesis.

7.1.2 PART II

In this part, we have considered a scenario where the network can support the data flow with reliability and accuracy, thus neglecting issues such as transmission delays, data loss, bandwidth as well as noise. In practice, these issues are are also very important but require careful consideration of several technicalities. Nonetheless, we envision that some extensions are indeed possible along the same lines as in De Persis and Frasca (2013); Senejohnny et al. (2017) where we discuss aspects related to the quality of the transmission medium.

Our approach utilizes a self-triggered update scheme with control saturation. It is of interest to investigate if similar results can be obtained also with event-triggered or other types of aperiodic update schemes e.g., Hetel et al. (2017); Dimarogonas et al. (2012). It is also interesting to see if similar results can be obtained with other averaging functions, for example with the classic coupling law for *average* consensus Cortés (2006). We envision an application of the present research within the context of distributed optimization of Sundaram and Gharesifard (2015, 2018), with specific reference to self-triggered schemes Fazlyab et al. (2016). Another interesting research venue is in the area of multi-agent systems with cloud access Nowzari and Pappas (2016). Also in this context, self-triggered control seems a viable option for enabling asynchronous coordination without destroying regulation properties.

Bibliography

W. Abbas, Y. Vorobeychik, and X. Koutsoukos, "Resilient consensus protocol in the presence of trusted nodes," in *International Symposium on Resilient Control Systems*. IEEE, 2014.

W. Abbas, A. Laszka, and X. Koutsoukos, "Improving network connectivity and robustness using trusted nodes with application to resilient consensus," *IEEE Transactions on Control of Network Systems*, 2017.

S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *International Workshop on Hybrid Systems: Computation and Control*. Springer, 2009, pp. 31–45.

M. Arcak, "Passivity as a design tool for group coordination," *IEEE Transactions on Automatic Control*, vol. 52, no. 8, pp. 1380–1390, 2007.

C.-Z. Bai, F. Pasqualetti, and V. Gupta, "Security in stochastic control systems: Fundamental limitations and performance bounds," in *American Control Conference (ACC), 2015*. IEEE, 2015, pp. 195–200.

C.-Z. Bai, F. Pasqualetti, and V. Gupta, "Data-injection attacks in stochastic control systems: Detectability and performance tradeoffs," *Automatica*, vol. 82, pp. 251–260, 2017.

H. Bai, M. Arcak, and J. Wen, *Cooperative control design: a systematic, passivity-based approach*. Springer Science & Business Media, 2011.

G. K. Befekadu, V. Gupta, and P. J. Antsaklis, "Risk-sensitive control under a class of denial-of-service attack models," in *American Control Conference (ACC), 2011*. IEEE, 2011, pp. 643–648.

J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions." in *USENIX security symposium*, vol. 12. Washington DC, 2003, pp. 2–2.

Y. Cao, W. Yu, W. Ren, and G. Chen, "An overview of recent progress in the study of distributed multi-agent coordination," *IEEE Transactions on Industrial informatics*, vol. 9, no. 1, pp. 427–438, 2013.

A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Distributed Computing Systems Workshops, 2008. ICDCS'08. 28th International Conference on*. IEEE, 2008, pp. 495–500.

A. Cetinkaya, H. Ishii, and T. Hayakawa, "Event-triggered control over unreliable networks subject to jamming attacks," *arXiv preprint arXiv:1503.06980*, 2015.

A. Cetinkaya, H. Ishii, and T. Hayakawa, "Networked control under random and malicious packet losses," *IEEE Transactions on Automatic Control*, vol. 62, no. 5, pp. 2434–2449, 2017.

A. Cetinkaya, H. Ishii, and T. Hayakawa, "Analysis of stochastic switched systems with application to networked control under jamming attacks," *IEEE Transactions on Automatic Control*, 2018.

A. Cetinkaya, H. Ishii, and T. Hayakawa, "The effect of time-varying jamming interference on networked stabilization," *SIAM Journal on Control and Optimization*, vol. 56, no. 3, pp. 2398–2435, 2018.

J. Cortés, "Finite-time convergent gradient flows with applications to network consensus," *Automatica*, vol. 42, no. 11, pp. 1993–2000, 2006.

C. De Persis and R. Postoyan, "A Lyapunov redesign of coordination algorithms for cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 2, pp. 808–823, 2017.

C. De Persis, "On self-triggered synchronization of linear systems," *IFAC Proceedings Volumes*, vol. 46, no. 27, pp. 247–252, 2013.

C. De Persis and P. Frasca, "Robust self-triggered coordination with ternary controllers," *IEEE Transactions on Automatic Control*, vol. 58, no. 12, pp. 3024–3038, 2013.

C. De Persis and P. Tesi, "Resilient control under denial-of-service," *IFAC Proceedings Volumes*, vol. 47, no. 3, pp. 134–139, 2014.

C. De Persis and P. Tesi, “Input-to-state stabilizing control under denial-of-service,” *IEEE Transactions on Automatic Control*, vol. 60, no. 11, pp. 2930–2944, 2015.

C. De Persis and P. Tesi, “Networked control of nonlinear systems under denial-of-service,” *Systems & Control Letters*, vol. 96, pp. 124–131, 2016.

C. De Persis and P. Tesi, “A comparison among deterministic packet-dropouts models in networked control systems,” *IEEE Control Systems Letters*, vol. 2, no. 1, pp. 109–114, 2018.

B. DeBruhl and P. Tague, “Digital filter design for jamming mitigation in 802.15. 4 communication,” in *Computer Communications and Networks (IC-CCN), 2011 Proceedings of 20th International Conference on*. IEEE, 2011, pp. 1–6.

S. M. Dibaji and H. Ishii, “Resilient consensus of second-order agent networks: Asynchronous update rules with delays,” *Automatica*, vol. 81, pp. 123–132, 2017.

S. M. Dibaji and H. Ishii, “Consensus of second-order multi-agent systems in the presence of locally bounded faults,” *Systems & Control Letters*, vol. 79, pp. 23–29, 2015.

S. M. Dibaji, H. Ishii, and R. Tempo, “Resilient randomized quantized consensus,” *IEEE Transactions on Automatic Control*, vol. PP, pp. 1–1 (In press), 2017.

D. V. Dimarogonas, E. Frazzoli, and K. H. Johansson, “Distributed event-triggered control for multi-agent systems,” *IEEE Transactions on Automatic Control*, vol. 57, no. 5, pp. 1291–1297, 2012.

D. Dolev, N. A. Lynch, S. S. Pinter, E. W. Stark, and W. E. Weihl, “Reaching approximate agreement in the presence of faults,” *Journal of the ACM*, vol. 33, no. 3, pp. 499–516, 1986.

V. Dolk, P. Tesi, C. De Persis, and W. Heemels, “Event-triggered control systems under denial-of-service attacks,” *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 93–105, 2017.

H. Fawzi, P. Tabuada, and S. Diggavi, “Secure state-estimation for dynamical systems under active adversaries,” in *Communication, Control, and Computing (Allerton), 2011 49th Annual Allerton Conference on*. IEEE, 2011, pp. 337–344.

H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic Control*, vol. 59, no. 6, pp. 1454–1467, 2014.

M. Fazlyab, C. Nowzari, G. J. Pappas, A. Ribeiro, and V. M. Preciado, "Self-triggered time-varying convex optimization," in *55th Conference on Decision and Control*. IEEE, 2016, pp. 3090–3097.

S. Feng and P. Tesi, "Resilient control under denial-of-service: Robust design," *Automatica*, vol. 79, pp. 42–51, 2017.

H. S. Foroush and S. Martinez, "On event-triggered control of linear systems under periodic denial-of-service jamming attacks," in *Decision and Control (CDC), 2012 IEEE 51st Annual Conference on*. IEEE, 2012, pp. 2551–2556.

M. Franceschelli, A. Giua, and A. Pisano, "Finite-time consensus on the median value with robustness properties," *IEEE Transactions on Automatic Control*, vol. 62, no. 4, pp. 1652–1667, 2017.

C. Godsil and G. Royle, *Algebraic Graph Theory*. Springer-Verlag New York, 2001.

A. Gupta, C. Langbort, and T. Başar, "Optimal control in the presence of an intelligent jammer with limited actions," in *Decision and Control (CDC), 2010 49th IEEE Conference on*. IEEE, 2010, pp. 1096–1101.

W. Heemels, K. H. Johansson, and P. Tabuada, "An introduction to event-triggered and self-triggered control," in *Decision and Control (CDC), 2012 IEEE 51st Annual Conference on*. IEEE, 2012, pp. 3270–3285.

J. P. Hespanha and A. S. Morse, "Stability of switched systems with average dwell-time," in *Decision and Control, 1999. Proceedings of the 38th IEEE Conference on*, vol. 3. IEEE, 1999, pp. 2655–2660.

L. Hetel, C. Fiter, H. Omran, A. Seuret, E. Fridman, J. Richard, and S. I. Niculescu, "Recent developments on the stability of systems with aperiodic sampling: An overview," *Automatica*, vol. 76, pp. 309–3350, 2017.

A. Jadbabaie, J. Lin, and A. S. Morse, "Coordination of groups of mobile autonomous agents using nearest neighbor rules," *IEEE Transactions on automatic control*, vol. 48, no. 6, pp. 988–1001, 2003.

E. D. Knapp and J. T. Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Syngress Publishing, 2011.

E. D. Knapp and R. Samani, *Applied Cyber Security and the Smart Grid*. Syngress Publishing, 2013.

H. J. LeBlanc and X. Koutsoukos, "Resilient asymptotic consensus in asynchronous robust networks," in *50th Annual Allerton Conference on Communication, Control, and Computing*. IEEE, 2012, pp. 1742–1749.

H. J. LeBlanc and X. Koutsoukos, "Resilient first-order consensus and weakly stable, higher order synchronization of continuous-time networked multiagent systems," *IEEE Transactions on Control of Network Systems*, 2017.

H. J. LeBlanc, H. Zhang, X. Koutsoukos, and S. Sundaram, "Resilient asymptotic consensus in robust networks," *IEEE Journal on Selected Areas in Communications,*, vol. 31, no. 4, pp. 766–781, 2013.

A.-Y. Lu and G.-H. Yang, "Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial of service," *IEEE Transactions on Automatic Control*, vol. 63, no. 6, pp. 1813–1820, 2018.

N. A. Lynch, *Distributed Algorithms*. Morgan Kaufmann, 1996.

T. Macaulay, *RIoT Control: Understanding and Managing Risks and the Internet of Things*. Morgan Kaufmann, 2016.

T. Macaulay and B. L. Singer, *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS*. Auerbach Publications, 2016.

Y. Mo and B. Sinopoli, "On the performance degradation of cyber-physical systems under stealthy integrity attacks," *IEEE Transactions on Automatic Control*, vol. 61, no. 9, pp. 2618–2624, 2016.

Y. Mo, S. Weerakkody, and B. Sinopoli, "Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs," *IEEE Control Systems*, vol. 35, no. 1, pp. 93–109, 2015.

C. Nowzari and G. J. Pappas, "Multi-agent coordination with asynchronous cloud access," in *2016 American Control Conference*. IEEE, 2016, pp. 4649–4654.

C. Nowzari, J. Cortes, and G. J. Pappas, "Event-triggered communication and control for multi-agent average consensus," *Cooperative Control of Multi-Agent Systems: Theory and Applications*, p. 177, 2017.

R. Olfati-Saber and R. M. Murray, "Consensus problems in networks of agents with switching topology and time-delays," *IEEE Transactions on automatic control*, vol. 49, no. 9, pp. 1520–1533, 2004.

F. Pasqualetti, F. Dorfler, and F. Bullo, "Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems," *IEEE Control Systems*, vol. 35, no. 1, pp. 110–127, 2015.

K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Communications surveys & tutorials*, vol. 13, no. 2, pp. 245–257, 2011.

R. Postoyan, P. Tabuada, D. Nešić, and A. Anta, "A framework for the event-triggered stabilization of nonlinear systems," *IEEE Transactions on Automatic Control*, vol. 60, no. 4, pp. 982–996, 2015.

R. Radvanovsky and J. Brodsky, *Handbook of SCADA/control systems security*. CRC Press, 2016.

D. Saldaña, A. Prorok, S. Sundaram, M. F. M. Campos, and V. Kumar, "Resilient consensus for time-varying networks of dynamic agents," in *2017 American Control Conference*. IEEE, 2017, pp. 2378–5861.

H. Sandberg, S. Amin, and K. H. Johansson, "Cyberphysical security in networked control systems: An introduction to the issue," *IEEE Control Systems*, vol. 35, no. 1, pp. 20–23, 2015.

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

D. Senejohnny, S. Sundaram, C. De Persis, and P. Tesi, "Resilience against misbehaving nodes in asynchronous networks," *Automatica, Provisionally accepted as Brief Paper*, 2018.

D. Senejohnny, S. Sundaram, C. De Persis, and P. Tesi, "Resilience against misbehaving nodes in self-triggered networks," in *Decision and Control (CDC), 2018 IEEE 57th Conference on*. IEEE, 2018.

D. Senejohnny, S. Sundaram, C. De Persis, and P. Tesi, "Misbehavior-resilient asymptotic coordination in asynchronous networks," *Under Prepration*, 2018.

D. Senejohnny, P. Tesi, and C. De Persis, "Self-triggered coordination over a shared network under denial-of-service," in *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*. IEEE, 2015, pp. 3469–3474.

D. Senejohnny, P. Tesi, and C. De Persis, "Resilient self-triggered network synchronization," in *Decision and Control (CDC), 2016 IEEE 55th Conference on*. IEEE, 2016, pp. 489–494.

D. Senejohnny, P. Tesi, and C. De Persis, "A jamming-resilient algorithm for self-triggered network coordination," *IEEE Transactions on Control of Network Systems, In Press*, 2017.

D. Senejohnny, P. Tesi, and C. De Persis, "Resilient self-triggered network synchronization," in *Control Subject to Computational and Communication Constraints*, S. Tarbouriech, A. Girard, and L. Hetel, Eds. Springer International Publishing, 2018, ch. 11.

D. Shi, Z. Guo, K. H. Johansson, and L. Shi, "Causality countermeasures for anomaly detection in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 63, no. 2, pp. 386–401, 2018.

R. S. Smith, "Covert misappropriation of networked control systems: Presenting a feedback structure," *IEEE Control Systems*, vol. 35, no. 1, pp. 82–92, 2015.

S. Sundaram and B. Gharesifard, "Consensus-based distributed optimization with malicious nodes," in *53rd Annual Allerton Conference on Communication, Control, and Computing*. IEEE, 2015, pp. 244–249.

S. Sundaram and B. Gharesifard, "Distributed optimization under adversarial nodes," *IEEE Transactions on Automatic Control*, 2018.

P. Tague, M. Li, and R. Poovendran, "Mitigation of control channel jamming under node capture attacks," *IEEE Transactions on Mobile Computing*, vol. 8, no. 9, pp. 1221–1234, 2009.

A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.

A. Teixeira, K. C. Sou, H. Sandberg, and K. H. Johansson, "Secure control systems: A quantitative risk management approach," *IEEE Control Systems*, vol. 35, no. 1, pp. 24–45, 2015.

D. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11 b and other networks," in *Proc. of MILCOM*, vol. 6, 2006, p. 100.

J. Usevitch and D. Panagou, "r-robustness and (r,s)-robustness of circulant graphs," in *arxiv.org/abs/1710.01990*, 2017.

N. H. Vaidya, L. Tseng, and G. Liang, "Iterative approximate byzantine consensus in arbitrary directed graphs," in *ACM Symposium on Principles of Distributed Computing*. IEEE, 2012, pp. 365–374.

M. Velasco, J. Fuertes, and P. Marti, "The self triggered task model for real-time control systems," in *Work-in-Progress Session of the 24th IEEE Real-Time Systems Symposium (RTSS03)*, vol. 384, 2003.

A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *computer*, vol. 35, no. 10, pp. 54–62, 2002.

W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*. ACM, 2005, pp. 46–57.

W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *IEEE network*, vol. 20, no. 3, pp. 41–47, 2006.

H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Transactions on Automatic Control*, vol. 60, no. 11, pp. 3023–3028, 2015.

M. Zhu and S. Martínez, "On the performance analysis of resilient networked control systems under replay attacks," *IEEE Transactions on Automatic Control*, vol. 59, no. 3, pp. 804–808, 2014.

Summary

With the advent of new concepts like Internet of Things (IoT), Industry 4.0, Smart Cities, and Smart Grid, new opportunities are brought into several industrial and societal domains ranging from transportation and electric power generation to traffic flow management and health care. Many of the above mentioned sectors and industries are essential to the health, safety, and security of our society and are considered critical infrastructure. This emphasizes the importance of rendering such systems "resilient" against malfunctioning due to genuine failures or cyberattacks.

Real-time availability and integrity of data are crucial to ensure normal operation of the system. The first factor is related to to the fact that data flow can be occasionally interrupted, while the second factor is related to the fact that the data content might be corrupted. Given these important factors, this thesis investigates the problem of designing coordination protocols over digital communication channels, which are resilient against the lack of data and unreliable information. The results are divided in two parts.

Part I is concerned with resilience against the absence of data and information accessibility due to genuine failure or cyberattacks, which results in Denial-of-Service (DoS). In particular, we are concerned with jamming attacks as we are mainly interested in wireless sensor networks. We design resilient consensus and synchronization protocols for both shared and peer-to-peer communication networks.

Part II is concerned with resilience against unreliable information in the network which could be the result of genuine fault/error in the control system operation or cyberattack. The nodes that communicate untrustworthy data in the network are considered misbehaving. We investigate a resilient consensus protocol against several types of misbehavior resulting from errors in operations such as data acquisition, data transmission, control logic, and update time scheduler.

Samenvatting

Met de opkomst van nieuwe concepten als Internet of Things, Industry 4.0, Smart Cities en Smart Grids ontstaan er nieuwe mogelijkheden in industriële en maatschappelijke sectoren, van transport en het opwekken van stroom tot verkeersregeling en gezondheidszorg. Veel van deze sectoren zijn essentieel voor de gezondheid en veiligheid van onze maatschappij en behoren tot de zogenoemde kritieke infrastructuur. Daaruit blijkt het belang om zulke systemen bestand te maken tegen problemen veroorzaakt door defecten of cyberaanvallen.

Beschikbaarheid en integriteit van data zijn cruciaal om zulke systemen goed te laten werken. Deze twee factoren kunnen in het geding komen vanwege het feit dat communicatiekanalen soms tijdelijk niet werken, respectievelijk het feit dat data tijdens het transport beschadigd of veranderd kan worden. Vanwege deze factoren behandelt dit proefschrift de uitdaging van het ontwerpen van coördinatieprotocols over digitale communicatiekanalen, die bestand zijn tegen datagebrek en foutieve data. De resultaten zijn opgedeeld in twee delen.

Deel I behandelt bestendigheid tegen de afwezigheid van data als gevolg van defecten of cyberaanvallen die resulteren in *Denial-of-Service*. In het bijzonder houden we ons bezig met aanvallen waarbij een draadloos communicatiekanaal verstoord wordt. We ontwerpen bestendige consensus- en synchronisatieprotocollen voor zowel gedeelde als peer-to-peernetwerken.

Deel II behandelt bestendigheid tegen onbetrouwbaarheid van de informatie in het netwerk, mogelijk als gevolg van een defect in het regelsysteem of een cyberaanval. De nodes in het netwerk die onbetrouwbare data aanleveren worden aangemerkt als zich misdragend. We onderzoeken een consensusprotocol dat bestand is tegen verschillende soorten misdragingen die het gevolg zijn van problemen bij dataverzameling, communicatie, aansturing en updateplanning.