Chapter 11
Resilient Self-Triggered Network Synchronization

D. Senejohnny, P. Tesi and C. De Persis

Abstract In this chapter, we investigate Self-Triggered synchronization of linear oscillators in the presence of communication failures caused by denial-of-Service (DoS). 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. A numerical example is given to substantiate the analysis.

11.1 Introduction

Cyber-physical systems (CPSs) exhibit a tight conjoining of computational and physical components. The fact that any breach in the cyberspace can have a tangible effect on the physical world has recently triggered attention toward cybersecurity also within the engineering community [1, 2]. In CPSs, attacks to the cyber-layer are mainly categorized as either denial-of-service (DoS) attacks or deception attacks. The latter affects the reliability of data by manipulating the transmitted packets over network; see [3, 4]. On the other hand, DoS attacks are primarily intended to affect the timeliness of the information exchange, i.e., to cause packet losses; see for instance [5, 6] for an introduction to the topic. This chapter aims at considering the effect of DoS attacks.

D. Senejohnny (✉) · P. Tesi · C. De Persis
ENTEG and Jan C. Willems Center for Systems and Control,
University of Groningen,
9747 AG Groningen, The Netherlands
e-mail: d.senejohnny@rug.nl

C. De Persis
e-mail: c.de.persis@rug.nl

P. Tesi
DINFO, Università degli Studi di Firenze, 50139 Firenze, Italy
e-mail: pietro.tesi@unifi.it; p.tesi@rug.nl

S. Tarbouriech et al. (eds.), *Control Subject to Computational and Communication Constraints*, Lecture Notes in Control and Information Sciences 475, https://doi.org/10.1007/978-3-319-78449-6_11

In the literature, the issue of resilience against DoS has been mostly investigated in *centralized* settings [7–14]. Very recently, [15, 16] explored this problem in a *distributed* setting with emphasis on consensus-like networks. The main goal of this chapter is to address the issue of resilience against DoS for network coordination problems in which node dynamics are more general than simple integrators. Specifically, we study *synchronization* networks of the same type as in [17]. Inspired by [18] and [19], we consider a *Self-Triggered* coordination scheme, in which the available information to each agent is used to update local controls and to specify the next update time. We consider Self-Triggered coordination schemes since they are of major interest when synchronization 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 coordination properties in the absence of any global information on the graph topology and with no need to resort to synchronous communication.

The primary step in the analysis of distributed coordination problems in the presence of DoS pertains to the modeling of DoS itself. In [12, 13], a general model is considered that only constrains DoS patterns in terms of their average frequency and duration. This makes it possible to describe a wide range of DoS-generating signals, e.g., trivial, periodic, random, and protocol-aware *jamming* [5, 6, 20, 21]. The occurrence of DoS has a different effect on the communication, depending on the network architecture. For networks operating through a single access point, in the so-called "infrastructure" mode, DoS may cause all the network links to fail simultaneously [15]. In this chapter, we consider instead a more general scenario in which the network links can fail independent of each other, thus extending the analysis to "ad-hoc" (peer-to-peer) network architectures. In this respect, a main contribution of this chapter is an explicit characterization of the frequency and duration of DoS at the various network links under which coordination can be preserved. In addition to extending the results of [19] to independent polling of neighbors, we also provide an explicit characterization of the effects of DoS on the coordination time. A preliminary and incomplete account of this work without the relevant proofs has appeared in [22].

The problem of network coordination under communication failures can be viewed as a coordination problem in the presence of switching topologies. For purely continuous-time systems, this problem has been thoroughly investigated under assumptions such as, point-wise, period-wise, and joint connectivity [23–25]. In CPSs, however, due to the presence of a digital communication layer, the situation is drastically different. In fact, the presence of a digital communication layer implies that the time span between any two consecutive transmissions cannot be arbitrarily small. As a consequence, the classic connectivity notions developed for purely continuous-time systems are not directly applicable to a digital setting as the one considered here. In this respect, we introduce a notion of *persistency-of-communication* (PoC), which requires graph (link) connectivity be be satisfied over periods of time that are consistent with the constraints imposed by the communication medium [15, 16].

The remainder of this chapter is organized as follows. In Sect. 11.2, we formulate the problem of interest and provide the results for Self-Triggered synchronization. In Sect. 11.3, we describe the considered class of DoS patterns. The main results are provided in Sect. 11.4. A numerical example is given in Sect. 11.5. Finally, Sect. 11.6 ends the chapter with concluding remarks.

Notation: The following notation is used throughout this chapter. The stacking of N column vectors $x_1, x_2, \ldots, x_n$ is denoted by x, i.e., $x = \left[x_1^\top \; x_2^\top \; \ldots \; x_n^\top\right]^\top$. The N- dimensional identity matrix is denoted by I_N. Vectors of all ones and zeros are denoted by $\mathbf{1}$ and $\mathbf{0}$, respectively. The ℓth component of vector x is denoted by x_ℓ or, interchangeably, by $[x]_\ell$.

11.2 Self-Triggered Synchronization

11.2.1 System Definition

We consider a connected and undirected graph $\mathscr{G} = (\mathscr{I}, \mathscr{E})$, where $\mathscr{I} := \{1, 2, \cdots, N\}$ is the set of nodes and $\mathscr{E} \subseteq \mathscr{I} \times \mathscr{I}$ is the set of links (edges). Given a node $i \in \mathscr{I}$, we shall denote by $\mathscr{N}_i = \{j \in \mathscr{I} : (i, j) \in \mathscr{E}\}$ the set of its neighbors, i.e., the set of nodes that exchange information with node i, and by $d^i = |\mathscr{N}_i|$, i.e., the cardinality of $\mathscr{N}_i$. 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 $\mathscr{G}$ 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

$$\dot{x}^i = Ax^i + Bu^i \tag{11.1}$$

where (A, B) is a stabilizable 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 $\mathscr{G}$. To achieve synchronization with constrained flow of information, we employ a hybrid controller with state variables $(x, \eta, \xi, \theta) \in \mathbb{R}^{n\times N} \times \mathbb{R}^{n\times N} \times \mathbb{R}^{n\times d} \times \mathbb{R}^{n\times d}$, where $d := \sum_{i=1}^{N} d^i$. The controller also makes use of a quantization function.

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

$$\text{sign}_\varepsilon(z) := \begin{cases} \text{sign}(z) & \text{if } |z| \geq \varepsilon \\ 0 & \text{otherwise} \end{cases} \tag{11.2}$$

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

$$\dot{\eta}^i = (A + BK)\eta^i + \sum_{j \in \mathscr{N}_i} \xi^{ij} \tag{11.3a}$$

$$\dot{\xi}^{ij} = A\xi^{ij} \tag{11.3b}$$

$$\dot{\theta}^{ij} = -\mathbf{1} \tag{11.3c}$$

$$u^i = K\eta^i, \tag{11.3d}$$

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 $(i, j) \in \mathscr{E}$, 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

$$\mathscr{S}(\theta, t) := \{(i, j, \ell) \in \mathscr{I} \times \mathscr{I} \times \mathscr{L} : \theta^{ij}_\ell(t^-) = 0\} \tag{11.4}$$

is nonempty, 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 $\ell \in \mathscr{L} := \{1, 2, \ldots, n\}$. At these time instants, in the "nominal" operating mode, a discrete transition (jump) occurs, which is given by

$$\begin{aligned}
x^i_\ell(t) &= x^i_\ell(t^-) \\
\eta^i_\ell(t) &= \eta^i_\ell(t^-) \\
\xi^{ij}_\ell(t) &= \begin{cases} [e^{At}\,\mathrm{sign}_\varepsilon(e^{-At}\mathscr{D}^{ij}(\eta(t) - x(t)))]_\ell & \text{if } (i, j, \ell) \in \mathscr{S}(\theta, t) \\ \xi^{ij}_\ell(t^-) & \text{otherwise} \end{cases} \\
\theta^{ij}_\ell(t) &= \begin{cases} f^{ij}_\ell(t) & \text{if } (i, j, \ell) \in \mathscr{S}(\theta, t) \\ \theta^{ij}_\ell(t^-) & \text{otherwise} \end{cases}
\end{aligned} \tag{11.5}$$

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

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

$$f^{ij}_\ell(x) = \max\left\{ \frac{\left|\left[e^{-At}\mathscr{D}^{ij}(\eta(t) - x(t))\right]_\ell\right|}{2(d^i + d^j)}, \frac{\varepsilon}{2(d^i + d^j)} \right\}. \tag{11.6}$$

Note that for all $(i, j) \in \mathscr{E}$ we have $\theta^{ij}(t) = \theta^{ji}(t)$ and $\xi^{ij}(t) = -\xi^{ji}(t)$ for all $t \in \mathbb{R}_{\geqslant 0}$. As such, (11.1)–(11.5) can be regarded as an edge-based synchronization protocol. Here, the term "Self-Triggered", first adopted in the context of real-time systems [26], 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 11.1 (*Controller structure*) The controller emulates the node dynamics (11.1), with an extra coupling term as done in [17]. The coupling is through the variable ξ^{ij}, which is updated at discrete times and emulates the open-loop behavior of (11.1) during its the controller continuous evolution [19]. Slightly different from [17], 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 (11.2) which triggers at discrete instances. ■

Remark 11.2 (*Clock variable θ_ℓ^{ij}*) Each clock variable θ_ℓ^{ij} plans ahead the update time of component ℓ of controller state ξ^{ij}. Whenever θ_ℓ^{ij} reaches zero, the ℓth 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 (11.6). In particular, this implies that for every edge $(i, j) \in \mathscr{E}$ and for any time $\mathscr{T}$, no more than $n\lfloor \frac{2(d^i+d^j)\mathscr{T}}{\varepsilon} + 1\rfloor$ number of updates can occur over an interval of length $\mathscr{T}$. ■

11.2.2 Practical Self-Triggered Synchronization

Inspired by [17], we analyze (11.1)–(11.5) using the change of coordinates

$$\begin{aligned} x^i(t) &= x^i(t) \\ \mathscr{X}^i(t) &= e^{-At}(\eta^i(t) - x^i(t)) \\ \mathscr{U}^{ij}(t) &= e^{-At}\xi^{ij}(t) \\ \theta^{ij}(t) &= \theta^{ij}(t). \end{aligned} \tag{11.7}$$

Accordingly, the network-state variables become $(x, \mathscr{X}, \mathscr{U}, \theta) \in \mathbb{R}^{n\times N} \times \mathbb{R}^{n\times N} \times \mathbb{R}^{n\times d} \times \mathbb{R}^{n\times d}$ with corresponding flow dynamics

$$\dot{x}^i(t) = (A + BK)x^i(t) + BKe^{At}\mathscr{X}^i(t) \tag{11.8a}$$

$$\begin{aligned} \dot{\mathscr{X}}^i(t) &= \sum_{j\in\mathscr{N}_i} \mathscr{U}^{ij} \\ \dot{\mathscr{U}}^{ij}(t) &= \mathbf{0} \\ \dot{\theta}^{ij}(t) &= -\mathbf{1} \end{aligned} \tag{11.8b}$$

and discrete transitions (jumps)

$$x_\ell^i(t) = x_\ell^i(t^-) \tag{11.9a}$$

$$\mathscr{X}_\ell^i(t) = \mathscr{X}_\ell^i(t^-)$$
$$\mathscr{U}_\ell^{ij}(t) = \begin{cases} \text{sign}_\varepsilon\,(\mathscr{D}_\ell^{ij}(\mathscr{X}(t)) & \text{if } (i,j,\ell) \in \mathscr{S}(\theta, t) \\ \\ \mathscr{U}_\ell^{ij}(t^-) & \text{otherwise} \end{cases} \tag{11.9b}$$
$$\theta_\ell^{ij}(t) = \begin{cases} g_\ell^{ij}(\mathscr{X}(t)) & \text{if } (i,j,\ell) \in \mathscr{S}(\theta, t) \\ \\ \theta_\ell^{ij}(t^-) & \text{otherwise} \end{cases}$$

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

$$g_\ell^{ij}(\mathscr{X}(t)) = \max\left\{ \frac{\left|\mathscr{D}_\ell^{ij}(\mathscr{X}(t))\right|}{2(d^i + d^j)}, \frac{\varepsilon}{2(d^i + d^j)} \right\}. \tag{11.10}$$

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 original synchronization problem into a consensus problem that involves integrator variables $\mathscr{X}^i$.

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

Theorem 11.1 (Practical Synchronization) *Let all the eigenvalues of A lie on the imaginary axis with geometric multiplicity equal to one. Let $(x, \mathscr{X}, \mathscr{U}, \theta)$ be the solution to system (11.8) and (11.9). Then, there exist a finite time T such that $\mathscr{X}$ converges within the time T to a point $\mathscr{X}_* = [\mathscr{X}_*^{1\top}, \ldots, \mathscr{X}_*^{N\top}]^\top$ in the set*

$$\mathscr{E} := \left\{ \mathscr{X} \in \mathbb{R}^{nN} : |\mathscr{D}_\ell^{ij}(\mathscr{X})| < \delta \;\; \forall (i,j,\ell) \in \mathscr{I} \times \mathscr{I} \times \mathscr{L} \right\}, \tag{11.11}$$

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

$$\left|x_\ell^i(t) - x_\ell^j(t)\right| < 2\varepsilon_c + \sqrt{n}\,\delta \;\; \forall (i,j,\ell) \in \mathscr{I} \times \mathscr{I} \times \mathscr{L} \tag{11.12}$$

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

Proof See the appendix. ■

Equations (11.11) and (11.12) involve a notion of "practical" 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 (11.6), the minimum inter-transmission time decreases with ε). Theorem 11.1 will be used as a reference frame for the analysis of Sect. 11.4. The case of asymptotic synchronization can be pursued along the lines of [18].

11.3 Network Denial-of-Service

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.

11.3.1 DoS Characterization

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

$$H_n^{ij} := \{h_n^{ij}\} \cup \left[h_n^{ij}, h_n^{ij} + \tau_n^{ij}\right[\tag{11.13}$$

represents the nth DoS time-interval, of a length $\tau_n^{ij} \in \mathbb{R}_{\geqslant 0}$, during which communication on the link (i, j) is not possible.

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

$$\Xi^{ij}(\tau, t) := \bigcup_{n\in\mathbb{Z}_{\geq 0}} H_n^{ij} \bigcap [\tau, t] \tag{11.14}$$

and

$$\Theta^{ij}(\tau, t) := [\tau, t] \setminus \Xi^{ij}(\tau, t) \tag{11.15}$$

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 [13], 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 11.2 (*DoS frequency*) For each $(i, j) \in \mathscr{E}$, there exist $\eta^{ij} \in \mathbb{R}_{\geq 0}$ and $\tau_f^{ij} \in \mathbb{R}_{>0}$ such that

$$n^{ij}(\tau, t) \leq \eta^{ij} + \frac{t-\tau}{\tau_f^{ij}} \tag{11.16}$$

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

Assumption 11.3 (*DoS duration*) For each $(i, j) \in \mathscr{E}$, there exist $\kappa^{ij} \in \mathbb{R}_{\geq 0}$ and $\tau_d^{ij} \in \mathbb{R}_{>1}$ such that

$$|\Xi^{ij}(\tau, t)| \leq \kappa^{ij} + \frac{t-\tau}{\tau_d^{ij}} \tag{11.17}$$

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

In Assumption 11.2, 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 η^{ij} is needed to render (11.16) self-consistent when $t = \tau = h_n^{ij}$ for some $n \in \mathbb{Z}_{\geqslant 0}$, in which case $n^{ij}(\tau, t) = 1$. Likewise, in Assumption 11.3, 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 η^{ij}, the constant κ^{ij} plays the role of a regularization term. It is needed because during a DoS interval, one has $|\Xi(h_n^{ij}, h_n^{ij} + \tau_n^{ij})| = \tau_n^{ij} \geqslant \tau_n^{ij}/\tau_d^{ij}$ 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 (11.17) self-consistent. Thanks to the quantities η^{ij} and κ^{ij}, DoS frequency and duration are both average quantities.

11.3.2 Discussion

The considered assumptions only pose limitations on the frequency of the DoS status and its duration. As such, this characterization can capture many different scenarios, including trivial, periodic, random and protocol-aware jamming [5, 6, 20, 21]. For the sake of simplicity, we limit our discussion to the case of radio frequency (RF) jammers, although similar considerations can be made with respect to spoofing-like threats [27].

Consider for instance the case of *constant jamming*, which is one of the most common threats that may occur in a wireless network [5, 28]. By continuously emitting RF signals on the wireless medium, this type of jamming can lower the packet send ratio (PSR) for transmitters employing carrier sensing as a 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 [21, 29]. 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 is nicely captured by the considered formulation.

As another example, consider the case of *reactive jamming* [5, 28]. 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 [29, 30]. Also, this case can be nicely accounted for via the considered assumptions.

11.4 Main Result

11.4.1 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,

$$
\begin{aligned}
x_\ell^i(t) &= x_\ell^i(t^-)\\
\mathscr{X}_\ell^i(t) &= \mathscr{X}_\ell^i(t^-)\\
\mathscr{U}_\ell^{ij}(t) &= \begin{cases} \mathrm{sign}_\varepsilon\,(\mathscr{D}_\ell^{ij}(\mathscr{X})) & \text{if } (i,j,\ell)\in\mathscr{S}(\theta,t)\wedge t\in\Theta^{ij}(0,t)\\ 0 & \text{if } (i,j,\ell)\in\mathscr{S}(\theta,t)\wedge t\in\Xi^{ij}(0,t)\\ \mathscr{U}_\ell^{ij}(t^-) & \text{otherwise}\end{cases}\\
\theta_\ell^{ij}(t) &= \begin{cases} g_\ell^{ij}(t) & \text{if } (i,j,\ell)\in\mathscr{S}(\theta,t)\wedge t\in\Theta^{ij}(0,t)\\ \dfrac{\varepsilon}{2(d^i+d^j)} & \text{if } (i,j,\ell)\in\mathscr{S}(\theta,t)\wedge t\in\Xi^{ij}(0,t)\\ \theta_\ell^{ij}(t^-) & \text{otherwise}\end{cases}
\end{aligned}
\tag{11.18}
$$

In words, the control action $\mathscr{U}^{ij}$ is reset to zero whenever the link (i,j) is in DoS status.[1] In addition to $\mathscr{U}$, also the local clocks are modified upon DoS, yielding a *two-mode* sampling logic. Let $\{t_{\ell_k}^{ij}\}_{\ell_k\in\mathbb{Z}_{\geq 0}}$ denote the sequence of transmission attempts for ℓth component of ξ^{ij} over the link $(i,j)\in\mathscr{E}$. Then, when a communication

[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.

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 (11.12), is preserved. This is achieved by resorting to a notion of persistency-of-Communication (PoC), which naturally extends the PoE condition [25] 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 11.1 (Convergence of the solutions) *Let $(x, \mathscr{X}, \mathscr{U}, \theta)$ be the solutions to (11.8) and (11.18). Then, there exists a finite time T_* such that, for any $(i, j) \in \mathscr{E}$, it holds that $\mathscr{U}^{ij}_{\ell}(t) = 0$ for all $\ell \in \mathscr{L}$ and for all $t \geqslant T_*$.*

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 $|\mathscr{X}^j_{\ell}(t) - \mathscr{X}^i_{\ell}(t)|$ 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 $\mathscr{X}^i(t) = \mathscr{X}^i(0)$ and the oscillator state $x^i(t)$ satisfies $\dot{x}^i(t) = Ax^i(t)$ with initial condition $-\mathscr{X}^i(0)$ for all $t \in \mathbb{R}_{\geqslant 0}$. In order to recover the same conclusions as in Theorem 11.1, bounds on DoS frequency and duration have to be enforced. The result which follows provides one such characterization. Let $(i, j) \in \mathscr{E}$ be a generic network link, and consider a DoS sequence on (i, j), which satisfies Assumptions 11.2 and 11.3. Define

$$\alpha^{ij} := \frac{1}{\tau^{ij}_d} + \frac{\Delta^{ij}_*}{\tau^{ij}_f} \tag{11.19}$$

where

$$\Delta^{ij}_* := \frac{\varepsilon}{2(d^i + d^j)}. \tag{11.20}$$

As for (ii), we have the following result.

Proposition 11.2 (Persistency-of-communication (PoC)) *Consider any link $(i, j) \in \mathscr{E}$ employing the transmission protocol* (11.18). *Also consider any DoS sequence on (i, j), which satisfies Assumptions 11.2 and 11.3 with η^{ij} and κ^{ij} arbitrary, and τ^{ij}_d and τ^{ij}_f such that $\alpha^{ij} < 1$. Let*

$$\Phi^{ij} := \frac{\kappa^{ij} + (\eta^{ij} + 1)\Delta^{ij}_*}{1 - \alpha^{ij}}. \tag{11.21}$$

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 11.1 to the presence of DoS.

Theorem 11.4 *Let* $(x, \mathscr{X}, \mathscr{U}, \theta)$ *be the solution to (11.8) and (11.18). For each* $(i, j) \in \mathscr{E}$*, consider any DoS sequence that satisfies Assumptions 11.2 and 11.3 with* η^{ij} *and* κ^{ij} *arbitrary, and* τ^{ij}_d *and* τ^{ij}_f *such that* $\alpha^{ij} < 1$*. Then,* $\mathscr{X}$ *converges in a finite time* T_* *to a point* $\mathscr{X}^*$ *in (11.11), and* $\mathscr{U}(t) = \mathbf{0}$ *for all* $t \geq T_*$*. Moreover, for every* $\varepsilon_c \in \mathbb{R}_{>0}$ *there exists a time* $T_c(\varepsilon_c) \geqslant T_*$ *such that (11.12) is satisfied for all* $t \geqslant T_c(\varepsilon_c)$.

Proof By Proposition 11.1, all the local controls become zero in a finite time T_*. In turn, Proposition 11.2 excludes that this is due to the persistence of a DoS status. Then the result follows along the same lines as in Theorem 11.1. ∎

Remark 11.3 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, [16] discusses how genuine DoS can be incorporated into this modeling framework. ∎

11.4.2 Effect of DoS on the Synchronization Time

By Theorem 11.4, $\dot{\mathscr{X}}$ 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 11.1 (Bound on the convergence time) *Consider the same assumptions as in Theorem 11.4. Then,*

$$T_* \leqslant \left[\frac{1}{\varepsilon} + \frac{d_{\max}}{\varepsilon d_{\min}} + \frac{4 d_{\max}}{\varepsilon^2}\Phi\right] \sum_{i \in \mathscr{I}} \sum_{\ell \in \mathscr{L}} (\eta^i_\ell(0) - x^i_\ell(0))^2, \tag{11.22}$$

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

Proof Consider the same Lyapunov function V as in the proof of Theorem 11.1. Notice that, by construction of the control law and the scheduling policy, for every successful transmission $t^{ij}_{\ell_k}$ characterized by $|\mathscr{D}^{ij}_\ell(\mathscr{X}(t^{ij}_{\ell_k})| \geqslant \varepsilon$, 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 $t^*_\ell \geqslant 0$ such that consensus has still not been reached on the ℓth component of $\mathscr{X}$. Note that we can have $\mathscr{U}^{ij}_\ell(t^*_\ell) = 0$ for all $(i, j) \in \mathscr{E}$. However, this condition can last only for a limited amount of time. In fact, if $\mathscr{U}^{ij}_\ell(t^*_\ell) = 0$ then the next transmission attempt, say l^{ij}_ℓ, over the link (i, j) and component-ℓ will necessarily occur at a time less than or equal to $t^*_\ell + \Delta^{ij}_*$ with $\Delta^{ij}_* \leqslant \varepsilon/(4d_{\min})$. Let $\mathscr{Q} := [t^*_\ell, t^*_\ell + \Delta^{ij}_*]$, and suppose that over $\mathscr{Q}$ some of the controls $\mathscr{U}^{ij}_\ell$ have remained equal to zero. This implies that for some $(i, j) \in \mathscr{E}$ we necessarily have that l^{ij}_ℓ is unsuccessful. This is because if $\mathscr{U}^{ij}_\ell(t) = 0$ for all $(i, j) \in \mathscr{E}$ and all $t \in \mathscr{Q}$ then $\mathscr{X}^i_\ell(t) = \mathscr{X}^i_\ell(t^*_\ell)$ for all $i \in \mathscr{I}$ and all $t \in \mathscr{Q}$. Hence, if all the l^{ij}_ℓ were successful, we should also have $\mathscr{U}^{ij}_\ell(l^{ij}_\ell) \neq 0$ for some $(i, j) \in \mathscr{E}$ since, by hypothesis, consensus is not reached at time t^*_ℓ. Hence, applying Proposition 11.2 we conclude that at least one of the controls $\mathscr{U}^{ij}_\ell$ will become nonzero before $l^{ij}_\ell + \Phi^{ij}$. As each vector component ℓ has the same Δ^{ij}_*, at least one of the control vectors $\mathscr{U}^{ij}$ will become nonzero 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

$$T_* \leqslant \left[\frac{\varepsilon}{4d_{\max}} + \frac{\varepsilon}{4d_{\min}} + \Phi\right]\frac{V(0)}{\varepsilon_*}. \tag{11.23}$$

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

$$V(0) = \frac{1}{2}\sum_{i\in\mathscr{I}}\sum_{\ell\in\mathscr{L}}(\mathscr{X}^i_\ell(0))^2. \tag{11.24}$$

■

11.5 A Numerical Example

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

Table 11.1 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 %

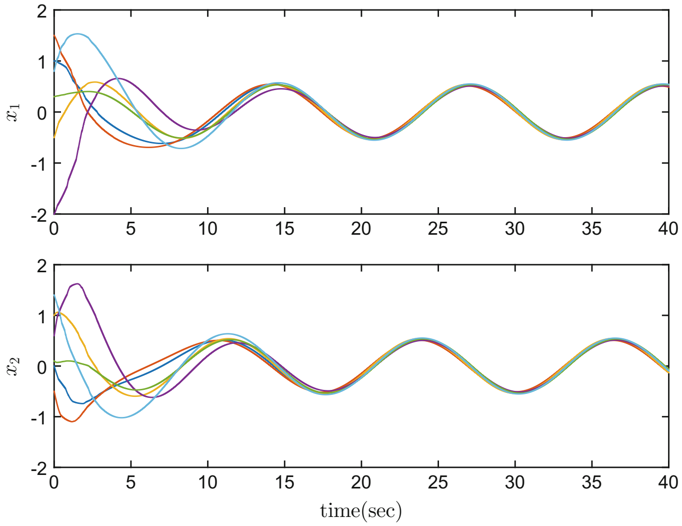

Fig. 11.1 Evolution of x, corresponding to the solution to (11.1)–(11.3) and (11.18) for a random graph with $N = 6$ nodes in the presence of DoS

$$\dot{x}^i(t) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} x^i(t) + \begin{bmatrix} 0 \\ 1 \end{bmatrix} u^i(t). \tag{11.25}$$

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

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 0.4sec and maximum duty cycle equal to 55%), both generated randomly. These patterns are reported in Table 11.1 for each network link.

The evolution of x, corresponding to the solutions to (11.1)–(11.3) and (11.18) with $\varepsilon = 0.04$ is depicted in Fig. 11.1. 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 Figs. 11.2 and 11.3. 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.

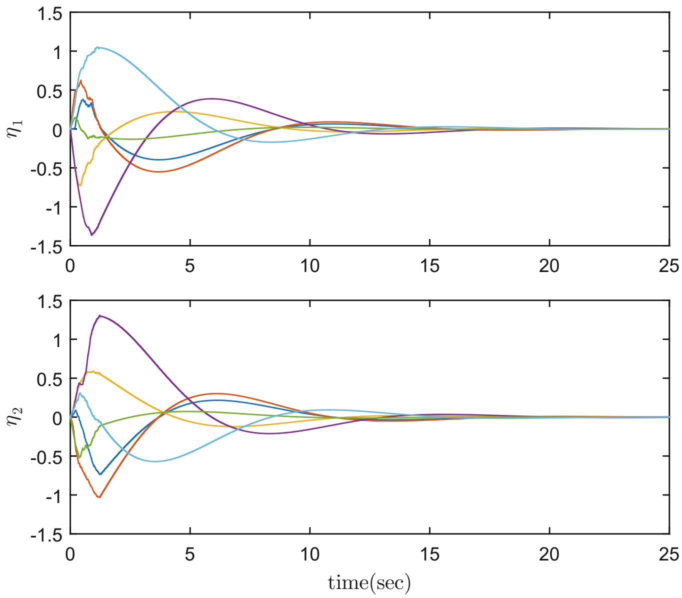

Fig. 11.2 Evolution of the controller state η in the absence of DoS

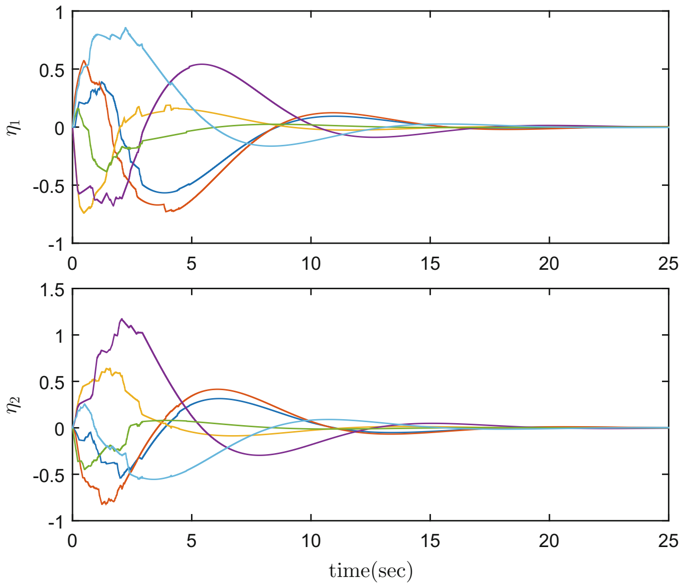

Fig. 11.3 Evolution of the controller state η in the presence of DoS

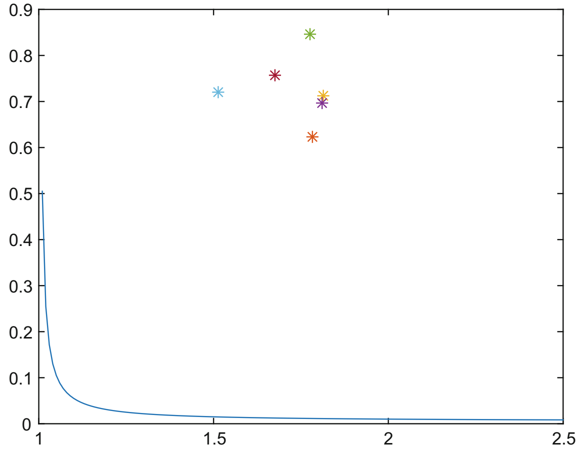

Fig. 11.4 Locus of the points $1/\tau_d + \Delta_*/\tau_f^{ij} = 1$ as a function of (τ_d, τ_f) with $\Delta_* = 0.05$ (blue solid line). The horizontal axis represents τ_d and the vertical axis represents τ_f. Notice that $\Delta_* = \Delta_*^{ij}$ for all $(i, j) \in \mathscr{E}$, so that the locus of point does not vary with (i, j). The various "$*$" represent the values of $(\tau_d^{ij}, \tau_f^{ij})$ for the network links

As a final comment, note that for each DoS pattern one can compute corresponding values for $(\eta^{ij}, \kappa^{ij}, \tau_f^{ij}, \tau_d^{ij})$. They can be determined by computing $n^{ij}(\tau, t)$ and $|\Xi^{ij}(\tau, t)|$ of each DoS pattern (cf. Assumptions 11.2 and 11.3) over the considered simulation horizon. Figure 11.4 depicts the values obtained for τ_f^{ij} and τ_d^{ij} for each $(i, j) \in \mathscr{E}$. One sees that these values are consistent with the requirements imposed by the PoC condition.

11.6 Conclusions

In this chapter, we have investigated Self-Triggered synchronization of group of harmonic oscillators in presence of denial-of-service at communication links. In the considered framework each of the network links fail independently, which is relevant for peer-to-peer networks architectures. A characterization of DoS frequency and duration is provided under which network synchronization is preserved, along with an explicit estimate of the effect of DoS on the time required to achieve synchronization.

Appendix

Proof of Theorem 11.1 As a first step, we analyze the consensus of subsystem $(\mathscr{X}, \mathscr{U}, \theta)$. Afterward, we will investigate the synchronization of the states x^i throughout the relation $\mathscr{X}^i(t) = e^{-At}(\eta^i(t) - x^i(t))$.

Consider the Lyapunov function $V(\mathscr{X}) = \frac{1}{2}\mathscr{X}^\top \mathscr{X}$, and let $t_{\ell_k}^{ij} := \max\{t_l^{ij} : t_l^{ij} \leqslant t, l \in \mathbb{Z}_{\geqslant 0}\}$. The derivative of V along the solutions to (11.8) satisfies

$$\begin{aligned}\dot{V}(\mathscr{X}(t)) &= \sum_{i=1}^{N} \mathscr{X}^{i\top}(t)\, \dot{\mathscr{X}}^{i}(t)\\ &= -\sum_{(i,j)\in\mathscr{E}} (\mathscr{X}^{j}(t)-\mathscr{X}^{i}(t))^{\top}\mathscr{U}^{ij}(t^{ij}_{\ell_k})\\ &= -\sum_{(i,j)\in\mathscr{E}}\sum_{\ell=1}^{n} \mathscr{D}^{ij}_{\ell}(\mathscr{X}(t))\,\mathrm{sign}_{\varepsilon}(\mathscr{D}^{ij}_{\ell}(\mathscr{X}(t^{ij}_{\ell_k}))).\end{aligned} \tag{11.26}$$

During the continuous evolution $|\dot{\mathscr{D}}^{ij}_{\ell}(\mathscr{X}(t))| \le d^i + d^j$ for $t \in [t^i_k, t^i_{k+1}[$, where $\mathscr{D}^{ij}(\mathscr{X}(t)) = \mathscr{X}^j(t) - \mathscr{X}^i(t)$. Exploiting this fact and recalling the definition of $g^{ij}_{\ell}(\mathscr{X}(t))$ in (11.10), it holds that if $|\mathscr{D}^{ij}_{\ell}(\mathscr{X}(t^{ij}_{\ell_k}))| \ge \varepsilon$ then

$$\begin{aligned}|\mathscr{D}^{ij}_{\ell}(\mathscr{X}(t))| &\ge |\mathscr{D}^{ij}_{\ell}(\mathscr{X}(t^{ij}_{\ell_k}))| - (d^i + d^j)(t - t^{ij}_{\ell_k})\\ &\ge \frac{|\mathscr{D}^{ij}_{\ell}(\mathscr{X}(t^{ij}_{\ell_k}))|}{2}\end{aligned} \tag{11.27}$$

and

$$\mathrm{sign}_{\varepsilon}(\mathscr{D}^{ij}_{\ell}(\mathscr{X}(t))) = \mathrm{sign}_{\varepsilon}(\mathscr{D}^{ij}_{\ell}(\mathscr{X}(t^{ij}_{\ell_k}))). \tag{11.28}$$

Using (11.27) and (11.28) we conclude that

$$\dot{V}(\mathscr{X}(t)) \le -\sum_{(i,j)\in\mathscr{E}} \sum_{\substack{\ell\in\mathscr{L}:\\ |\mathscr{D}^{ij}_{\ell}(\mathscr{X}(t^{ij}_{\ell_k}))|\ge\varepsilon}} \frac{|\mathscr{D}^{ij}_{\ell}(\mathscr{X}(t^{ij}_{\ell_k}))|}{2} \tag{11.29}$$

In view of (11.29), there must exist a finite time T such that, for every $(i, j) \in \mathscr{E}$ and every k, ℓ with $t^{ij}_{\ell_k} \geqslant T$, it holds that $|\mathscr{D}^{ij}_{\ell}(\mathscr{X}(t^{ij}_{\ell_k}))| < \varepsilon$. This is because, otherwise, V would become negative. The inequality in (11.11) follows by recalling that, in a graph with N nodes the graph diameter is $N - 1$. This shows that $\mathscr{X}$ converges in a finite time T to a point $\mathscr{X}_*$ in the set $\mathscr{E}$.

We now focus on x. In view of (11.2), $\mathscr{U}$ converges to zero in a finite time. Moreover, in view of (11.7), we have that $\eta^i(t) - x^i(t)$ converges to $e^{At}\mathscr{X}^i_*$ and ξ to $\mathbf{0}$ in a finite time. As for η, recall that η^i has flow and jump dynamics given by

$$\begin{aligned}\dot{\eta}^i(t) &= (A + BK)\eta^i(t) + \sum_{j\in\mathscr{N}_i} \xi^{ij}(t)\\ \eta^i(t) &= \eta^i(t^-).\end{aligned} \tag{11.30}$$

Hence, η converges exponentially to the origin since ξ converges to $\mathbf{0}$ 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 $e^{At}\mathscr{X}^i_*$, we have that $x^i(t)$ convergence asymptotically to

$-e^{At}\mathscr{X}_*^i$. This implies that for any node $i \in \mathscr{I}$ and any $\varepsilon_c \in \mathbb{R}_{>0}$, there exists a time $T_c(\varepsilon_c)$ after which $\|x^i(t) + e^{At}\mathscr{X}_*^i\| \le \varepsilon_c$, where $\|\cdot\|$ stands for Euclidean norm.

Notice that, in general, $\mathscr{X}_*^i \neq \mathscr{X}_*^j$ for $i \neq j$ in accordance with the practical consensus property (11.11). Therefore, the solutions x^i and x^j for all $(i, j) \in \mathscr{I} \times \mathscr{I}$ will achieve practical consensus as well. In particular, an upper bound on their disagreement level can be estimated as

$$\begin{aligned}\|x^i(t) - x^j(t)\| &\le \|x^i(t) + e^{At}\mathscr{X}_*^i\| + \|x^j(t) + e^{At}\mathscr{X}_*^i\| \\ &\leqslant \|x^i(t) + e^{At}\mathscr{X}_*^i\| + \|x^j(t) + e^{At}\mathscr{X}_*^j\| + \|e^{At}\mathscr{X}_*^i - e^{At}\mathscr{X}_*^j\| \\ &\le 2\varepsilon_c + \|e^{At}(\mathscr{X}_*^j - \mathscr{X}_*^i)\| \\ &\le 2\varepsilon_c + \sqrt{n}\,\delta\end{aligned} \tag{11.31}$$

where the last inequality is obtained from (11.11) and the fact that A has purely imaginary eigenvalues by hypothesis. This concludes the proof. ∎

Proof of Proposition 1 Reasoning as in the proof of Theorem 11.1, it is an easy matter to see that in the presence of DoS (11.29) modifies into

$$\dot{V}(\mathscr{X}(t)) \le - \sum_{(i,j)\in\mathscr{E}} \sum_{\substack{\ell\in\mathscr{L}: \\ |\mathscr{D}_\ell^{ij}(\mathscr{X}(t_{\ell_k}^{ij}))|\ge\varepsilon\,\wedge \\ t_{\ell_k}^{ij}\in\Theta^{ij}(0,t)}} \frac{|\mathscr{D}_\ell^{ij}(\mathscr{X}(t_{\ell_k}^{ij}))|}{2}. \tag{11.32}$$

In words, the derivative of V decreases whenever, for some $(i, j) \in \mathscr{E}$, $\ell \in \mathscr{L}$, two conditions are met: (i) $|\mathscr{D}_\ell^{ij}(\mathscr{X}(t_{\ell_k}^{ij}))| \geqslant \varepsilon$, 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 (11.32) there must exist a finite time T_* such that, for every $\{i, j, \ell\} \in \mathscr{E} \times \mathscr{L}$ and every k with $t_{\ell_k}^{ij} \geqslant T_*$, it holds that $|\mathscr{D}_\ell^{ij}(\mathscr{X}(t_{\ell_k}^{ij}))| < \varepsilon$ 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 $|\mathscr{D}_\ell^{ij}(\mathscr{X}(t_{\ell_k}^{ij}))| < \varepsilon$ and $t_{\ell_k}^{ij} \in \Xi^{ij}(0, t)$ the control $\mathscr{U}_\ell^{ij}(t)$ is set equal to zero. ∎

Proof of Proposition 11.2 Consider any link $(i, j) \in \mathscr{E}$, 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 nth DoS interval over the link (i, j) prolonged by Δ_*^{ij} units of time. Also, let

$$\bar{\Xi}^{ij}(\tau, t) := \bigcup_{n\in\mathbb{Z}_{\ge 0}} \bar{H}_n^{ij} \bigcap [\tau, t] \tag{11.33}$$

$$\bar{\Theta}^{ij}(\tau, t) := [\tau, t] \setminus \bar{\Xi}^{ij}(\tau, t). \tag{11.34}$$

Suppose then that the claim is false, and let $t^\star_\ell$ denote the last transmission attempt over $[t^{ij}_{\ell_k}, t^{ij}_{\ell_k} + \Phi^{ij}]$. Notice that this necessarily implies $|\bar{\Theta}^{ij}(t^{ij}_{\ell_k}, t^\star_\ell)| = 0$. To see this, first note that, in accordance with (11.18), the inter-sampling time over the interval $[t^{ij}_{\ell_k}, t^\star_\ell]$ is equal to $\varepsilon/(2(d^i + d^j)) = \Delta^{ij}_*$. Hence, we cannot have $|\bar{\Theta}^{ij}(t^{ij}_{\ell_k}, t^\star_\ell)| > 0$ since this would imply the existence of a DoS-free interval within $[t^{ij}_{\ell_k}, t^\star_\ell]$ of length greater than Δ^{ij}_*, which is not possible since, by hypothesis, no successful transmission attempt occurs within $[t^{ij}_{\ell_k}, t^\star_\ell]$. Thus $|\bar{\Theta}^{ij}(t^{ij}_{\ell_k}, t^\star_\ell)| = 0$. Moreover, since $t^\star_\ell$ is unsuccessful, it must be contained in a DoS interval, say H^{ij}_q. This implies $[t^\star_\ell, t^\star_\ell + \Delta^{ij}_*[\subseteq \bar{H}^{ij}_q$. Hence, we have

$$
\begin{aligned}
|\bar{\Theta}^{ij}(t^{ij}_{\ell_k}, t^\star_\ell + \Delta^{ij}_*)| &= |\bar{\Theta}^{ij}(t^{ij}_{\ell_k}, t^\star_\ell)| + |\bar{\Theta}^{ij}(t^\star_\ell, t^\star_\ell + \Delta^{ij}_*)| \\
&= 0
\end{aligned}
\tag{11.35}
$$

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

$$
\begin{aligned}
|\bar{\Theta}^{ij}(t^{ij}_{\ell_k}, t)| &= t - t^{ij}_{\ell_k} - |\bar{\Xi}^{ij}(t^{ij}_{\ell_k}, t)| \\
&\geqslant t - t^{ij}_{\ell_k} - |\Xi^{ij}(t^{ij}_{\ell_k}, t)| - (n(t^{ij}_{\ell_k}, t) + 1)\Delta^{ij}_* \\
&\geqslant (t - t^{ij}_{\ell_k})(1 - \alpha^{ij}) - \kappa^{ij} - (\eta^{ij} + 1)\Delta^{ij}_*
\end{aligned}
\tag{11.36}
$$

for all $t \geqslant t^{ij}_{\ell_k}$ where the first inequality follows from the definition of the set $\bar{\Xi}^{ij}(\tau, t)$ while the second one follows from Assumptions 11.2 and 11.3. Hence, by (11.36), we have $|\bar{\Theta}^{ij}(t^{ij}_{\ell_k}, t)| > 0$ for all $t > t^{ij}_{\ell_k} + (1 - \alpha^{ij})^{-1}(\kappa^{ij} + (\eta^{ij} + 1)\Delta^{ij}_*) = t^{ij}_{\ell_k} + \Phi^{ij}$. Accordingly, $|\bar{\Theta}(t^{ij}_{\ell_k}, t^\star_\ell + \Delta^{ij}_*)| = 0$ cannot occur because $t^\star_\ell + \Delta^{ij}_* > t^{ij}_{\ell_k} + \Phi^{ij}$. In fact, by hypothesis, $t^\star_\ell$ is defined as the last unsuccessful transmission attempt within $[t^{ij}_{\ell_k}, t^{ij}_{\ell_k} + \Phi^{ij}]$, and, by (11.18), the next transmission attempt after $t^\star_\ell$ occurs at time $t^\star_\ell + \Delta^{ij}_*$. This concludes the proof. ∎

References

1. Sandberg, H., Amin, S., Johansson, K.: Cyberphysical security in networked control systems: an introduction to the issue. IEEE Control Syst. **35**(1), 20–23 (2015)
2. Cardenas, A.A., Amin, S., Sastry, S.: Secure control: towards survivable cyber-physical systems. In: The 28th International Conference on Distributed Computing Systems Workshops, pp. 495–500 (2008)
3. Fawzi, H., Tabuada, P., Diggavi, S.: Secure state-estimation for dynamical systems under active adversaries. In: 2011 49th Annual Allerton Conference on Communication, Control, and Computing (Allerton), pp. 337–344 (2011)
4. Pasqualetti, F., Dorfler, F., Bullo, F.: Control-theoretic methods for cyberphysical security: geometric principles for optimal cross-layer resilient control systems. IEEE Control Syst. **35**(1), 110–127 (2015)

5. Xu, W., Ma, K., Trappe, W., Zhang, Y.: Jamming sensor networks: attack and defense strategies. IEEE Netw. **20**(3), 41–47 (2006)
6. Thuente, D., Acharya, M.: Intelligent jamming in wireless networks with applications to 802.11 b and other networks. In: Proceedings of the 25th IEEE Communications Society Military Communications Conference (MILCOM06), pp. 1–7. Washington, DC (2006)
7. Amin, S., Càrdenas, A., Sastry, S.: Safe and secure networked control systems under denial of-service attacks. In: Hybrid Systems: Computation and Control, pp. 31–45 (2009)
8. Gupta, A., Langbort, C., Basar, T.: Optimal control in the presence of an intelligent jammer with limited actions. In: Proceedings of the IEEE Conference on Decision and Control, pp. 1096–1101 (2010)
9. Befekadu, G., Gupta, V., Antsaklis, P.: Risk-sensitive control under a class denial-of-service attack models. In: 2011 American Control Conference. CA, USA, San Francisco (2011)
10. Teixeira, A., Shames, I., Sandberg, H., Johansson, K.H.: A secure control framework for resource-limited adversaries. Automatica **51**, 135–148 (2015)
11. Foroush, H.S., Martínez, S.: On event-triggered control of linear systems under periodic denial-of-service jamming attacks. In: Proceedings of the IEEE Conference on Decision and Control, pp. 2551–2556 (2012)
12. De Persis, C., Tesi, P.: Resilient control under denial-of-service. In: Proceedings of the IFAC World Conference. Cape Town, South Africa, pp. 134–139 (2013)
13. De Persis, C., Tesi, P.: Input-to-state stabilizing control under denial-of-service. IEEE Trans. Autom. Control **60**, 2930–2944 (2015)
14. De Persis, C., Tesi, P.: Networked control of nonlinear systems under denial-of-service. Syst. Control Lett. **96**, 124–131 (2016)
15. Senejohnny, D., Tesi, P., De Persis, C.: Self-triggered coordination over a shared network under denial-of-service. In: Proceedings of the IEEE Conference on Decision and Control, pp. 3469–3474. Osaka, Japan (2015)
16. Senejohnny, D., Tesi, P., De Persis, C.: A jamming-resilient algorithm for self-triggered network coordination. IEEE Trans. Control Netw. Syst. **PP**, 1–1 (2017). Inpress
17. Scardovi, L., Sepulchre, R.: Synchronization in networks of identical linear systems. Automatica **45**(11), 2557–2562 (2009)
18. De Persis, C., Frasca, P.: Robust self-triggered coordination with ternary controllers. IEEE Trans. Autom. Control **58**(12), 3024–3038 (2013)
19. De Persis, C.: On self-triggered synchronization of linear systems. Estim. Control Networked Syst. **4**(1), 247–252 (2013)
20. Xu, W., Trappe, W., Zhang, Y., Wood, T.: 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, pp. 46–57. ACM (2005)
21. Tague, P., Li, M., Poovendran, R.: Mitigation of control channel jamming under node capture attacks. IEEE Trans. Mob. Comput. **8**(9), 1221–1234 (2009)
22. Senejohnny, D., Tesi, P., De Persis, C.: Resilient self-triggered network synchronization. In: Proceedings of the IEEE Conference on Decision and Control, pp. 489–494. Las Vegas, USA (2016)
23. Olfati-Saber, R., Murray, R.M.: Consensus problems in networks of agents with switching topology and time-delays. IEEE Trans. Autom. Control **49**(9), 1520–1533 (2004)
24. Jadababaie, A., Lin, J., Morse, A.: Coordination of groups of mobile autonomous agents using nearest neighbour rules. IEEE Trans. Autom. Control **48**(6), 988–1001 (2003)
25. Arcak, M.: Passivity as a design tool for group coordination. IEEE Trans. Autom. Control **52**(8), 1380–1390 (2007)
26. Velasco, P.M.M., Fuertes, J.: The self-triggered task model for real-time control systems. In: Proceedings of 24th IEEE Real-Time Systems Symposium, Work-in-Progress Session (2003)
27. Bellardo, J., Savage, S.: 802.11 denial-of-service attacks: real vulnerabilities and practical solutions. In: USENIX security, pp. 15–28 (2003)
28. Pelechrinis, K., Iliofotou, M., Krishnamurthy, S.V.: Denial of service attacks in wireless networks: the case of jammers. IEEE Commun. Surv. Tutor. **13**(2), 245–257 (2011)

29. DeBruhl, B., Tague, P.: Digital filter design for jamming mitigation in 802.15. 4 communication. In: 2011 Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN), pp. 1–6 (2011)
30. Wood, A.D., Stankovic, J., et al.: Denial of service in sensor networks. Computer **35**(10), 54–62 (2002)