DIPARTIMENTO DI INGEGNERIA INFORMATICA
AUTOMATICA E GESTIONALE ANTONIO RUBERTI

SAPIENZA
UNIVERSITÀ DI ROMA

Control of Autonomous Multi-Agent Systems

Report

State of the Art on Resilient Output Regulation of Linear Systems Under Denial-of-Service Attacks by Event-Triggered Control and other relevant approaches

Ludovica Cartolano
cartolano.1796046@studenti.uniroma1.it

Supervised by
PhD Danilo Menegatti

Master in Control Engineering

Department of Computer, Control and Management Engineering
"Antonio Ruberti" (DIAG)
University of Rome "La Sapienza"
AY 2022/2023

Contents

List of Figures

Chapter 1

Introduction

In this report I investigate the state of the arts of resilient output regulation problem of systems under denial-of-service attacks through the different techniques showed in the articles [Chao Deng 2022], [Jiang 2022] and focusing in particular on the work of Yongjie Zhang and Chen 2023.

In the article [Chao Deng 2022] the authors discuss about the resilient practical cooperative output regulation for MASs with unknown switching exosystem dynamics under DoS attacks.
In the article [Jiang 2022] the authors discuss about the resilient reinforcement learning and robust output regulation under denial-of-service attacks.
Finally, in the article [Yongjie Zhang and Chen 2023] the authors discuss about the resilient output regulation problem of a linear system under denial-of-service attacks by event triggered control.

All these articles discuss some general features such as output regulation, denial-of-service attacks and event-triggered control.

Output Regulation Problem concerns with the design of a feedback law to impose a prescribed steady state response to every external command in a prescribed family. The case in the article [Yongjie Zhang and Chen 2023] covers the problem of having an output y(·) asymptotically rejecting a class of undesired disturbances while maintaining the internal stability of the closed loop system. The matter is to impose the so called tracking error, namely the difference between the reference output and the actual output, decays to zero at steady state [Isidori 1995]. For multi-agent systems (MASs) the control objective of the Cooperative Output Regulation Problem (CORP) is to build a distributed control protocol based on local and neighbor knowledge so that the regulated outputs tend to follow desired trajectories. The extra agent or the leader in the CORP is an exosystem that generates external signals to be tracked and/or rejected. The CORP's control objective is to track the reference trajectory generated by the leader and reject effect perturbations for MASs [Chao Deng 2022]. These concept have been generalised in the case of non-linear systems in [Dan, Chao, and Gang 2023].

The reliability of the communication network was guaranteed in the early research on the output regulation problem of network control systems. This can no longer be assured because, in recent years, the communication network has become increasingly vulnerable to hacker attacks, notably in Networked Control Systems (NCS) [Li 2022] and MASs [Chao Deng 2022]. The most common attack is the Denial-of-Service (DoS) attack. In DoS attacks the adversary aims to drop transmitted data packets, so that the performance of the closed loop is deteriorated, perhaps even unstable [Michelle S. Chong 2019]. In general these attacks do not need to know the model specifics and there is no need to break the confidentiality (disclosure resources); but the attacker is able to drop the transmitted data packets and block them from reaching the intended destination [Michelle S. Chong 2019].

In the cases of study the DoS it is intended to induce instability by maliciously jamming the bandwidth-limited channel. That is why on this scenario will be used an event-triggered control approach: if the attack problem satisfies some conditions then the problem is solvable by state feedback control scheme.

Event-triggered systems - or event-driven systems - are defined as discrete-state systems where the state takes values in a discrete set and changes due to the occurrence of an event [John Lygeros and Tomlin 2020].

Switched systems consist of a finite number of subsystems and a designated logical rule orchestrating the switching sequence among these sub-systems. Switching mechanisms provide more flexible options for system design, which has aroused wide attention to switched systems. In contrast, switched systems give an effective way to characterize multi-mode/multi-objective and strong nonlinear behavior [Li 2022]. Moreover, event-driven systems, are subject to Zeno Behavior, due to simplification assumptions on the model (A).

The paper [Jiang 2022] will address Reinforcement Learning (RL) as a development of prior RL-based stabilization approaches in which one has solved adaptive optimum output regulation problems so that the closed-loop system can asymptotically track the reference while rejecting the disturbance in a model-free optimal sense.

All theories of learning and intelligence start with the premise that humans learn by interaction. RL is a technique to machine learning that places more of an emphasis on goal-directed learning via interaction than other approaches. RL is the understanding of how to link events to behaviors in order to maximize a numerical reward signal. To achieve a goal, a learning agent must interact with its surroundings over time and identify the key elements of the genuine challenge it faces. In order to be rewarded, an agent must learn a set of rules about how to behave. The agent's objective is to develop a mapping of the environment and its properties based on its current observations [Sutton and Barto 2018].

Unlike classic RL, which only examines system static uncertainties, in [Jiang 2022] the authors use a new approach on robust adaptive dynamic programming (RADP) to solve system dynamic uncertainties by building a robust optimal controller.

For the notations please refer to the articles [Chao Deng 2022], [Jiang 2022] and [Yongjie Zhang and Chen 2023].

Chapter 2

Preliminaries

In this chapter, I shall proceed with the general formulation of the problems mentioned in each of the articles under consideration.

Assumption 1. *The indirected graph G is connected and at least one agent has access to the information of the exosystem state.*

Consider the linear system dynamics:

$$\begin{cases} \dot{x} = Ax + Bu + Ev \\ e = Cx + Du + Fv \end{cases} \tag{2.1}$$

where $x \in \mathbb{R}^n$ is the system state, $u \in \mathbb{R}^m$ is the control input and $e \in \mathbb{R}^p$ is the tracking error. The signal $v \in \mathbb{R}^q$ denotes the reference input to be tracked or even disturbances to be rejected and it is generated the following exosystem:

$$\dot{v} = Sv \tag{2.2}$$

where $S \in \mathbb{R}^{qxp}$ is a constant matrix.

The equations (2.1) and (2.2) can be used also in the case of [Chao Deng 2022] and [Jiang 2022]; in particular (2.1) models each dynamics of a MASs.

Consider now the DoS attack as it is defined in [Yongjie Zhang and Chen 2023]. Let $\{h_n\}_{n\in\mathbb{N}_0}$, where $h_0 \geq 0$, denote the sequence of DoS *off/on* transition, which are the time instants at which DoS exhibits a logical transition from 0 (communication is possible), to 1 (communication is interrupted). Define the nth DoS time-interval of a length $\tau_n \in \mathbb{R}_{\geq 0}$ over which communication is not possible

$$H_n := \{h_n\} \cup [h_n, h_n + \tau_n[\tag{2.3}$$

If $\tau_n = 0$, the nth DoS takes the form of a single pulse at time h_n. Given $\tau, t \in \mathbb{R}_{\geq 0}$, let

$$\Xi(\tau, t) := \bigcup_{n\in\mathbb{N}_0} H_n \bigcap [\tau, t] \tag{2.4}$$

$$\Theta(\tau, t) := [\tau, t] \backslash \Xi(\tau, t) \tag{2.5}$$

For each interval $[\tau, t]$, $\Xi(\tau, t)$ represents the set of time instants where communication is denied and $\Theta(\tau, t)$ is the set of time instants where communication is allowed. Please note that the attacker action in time has limitations on the frequency of DoS attacks and their duration that is why in the following some assumptions on the DoS will be articulated.

Assumption 2. *There exist $\eta \in \mathbb{R}_{>0}$ and $\tau_{\mathcal{D}}$ such that*

$$n(\tau, t) \leq \eta + \tfrac{t-\tau}{\tau_{\mathcal{D}}} \quad \forall\, \tau, t \in \mathbb{R}_{\geq 0} \; \textit{with} \; t \geq \tau$$

where $n(\tau,\ t)$ denotes the number of DoS off/on transitions occurring on the interval $[\ \tau, t]$ [Jiang 2022]. $\tau_{\mathcal{D}}$ is the average dwell time between consecutive off/on transitions while η is the chattering bound.

Assumption 3. *There exists a constant $\kappa \in \mathbb{R}_{\geq 0}$ and $T \in \mathbb{R}_{>1}$ such that*

$$|\Xi(\tau, t)| \leq \kappa + \tfrac{t-\tau}{T} \quad \forall\, \tau, t \in \mathbb{R}_{\geq 0} \; \textit{with} \; t \geq \tau$$

In other words on average, the total duration over which communication is interrupted does not exceed $1/T$ and the κ term has a regularization function.

The DoS formulation can be considered as it is also for [Chao Deng 2022] and [Jiang 2022].

Assumption 4. *The exosystem (2.2) is marginally stable. This means that all the eigenvalues of S are simple with zero real part (Jiang 2022).*

This guarantees the boundedness of the exogenous signal *v(t).*

Assumption 5. *The pair (A, B) of the plant (2.1) is stabilisable.*

Assumption 6. *The pair $\left(\begin{bmatrix} C & F \end{bmatrix}, \begin{bmatrix} A & E \\ 0 & S \end{bmatrix}\right)$ from the equations (2.1) and (2.2) is detectable.*

Assumption 5 and Assumption 6 are necessary conditions for the solvability of the output feedback control law.

Assumption 7. $\forall \lambda \in \sigma(S)$ *then*

$$rank \begin{bmatrix} A - \lambda I & B \\ C & D \end{bmatrix} = n + m$$

where n is the state dimension and m is the dimension of the control action.

This is also called the resonance condition and it is a necessary and sufficient condition to find a regulator equation (or Francis' equation). It guarantees that for any matrices E and F, the regulator equation associated with the systems (2.1) and (2.2),

$$\begin{aligned} XS &= AX + BU + E \\ 0 &= CX + DU + F \end{aligned} \tag{2.6}$$

has pair of solution (X, U).

Chapter 3

Main Results

Follows a brief discussion of the characteristics and main results of each study.

3.1 Resilient practical cooperative output regulation for MASs with unknown switching exosystem dynamics under DoS attacks

The article [Chao Deng 2022] produces a novel resilient practical cooperative output regulation control scheme. This scheme is composed by: a data-driven learning algorithm to estimate the unknown switching matrix, an auxiliary observer to estimate the state of the exosystem, distributed resilient observers to estimate the state of the auxiliary system and distributed controllers for individual agents. By using the dwell-time method, rigorous stability analysis shows that the resilient observation errors are globally ultimately bounded in the presence of DoS attacks and the resilient practical CORP is solved.

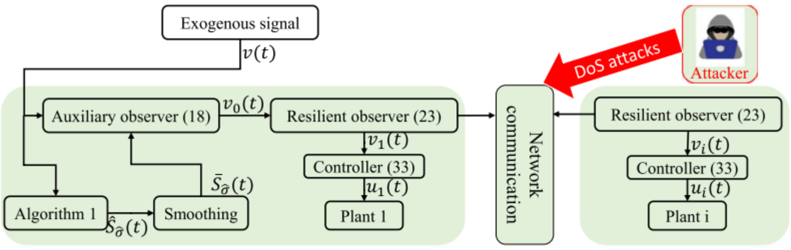
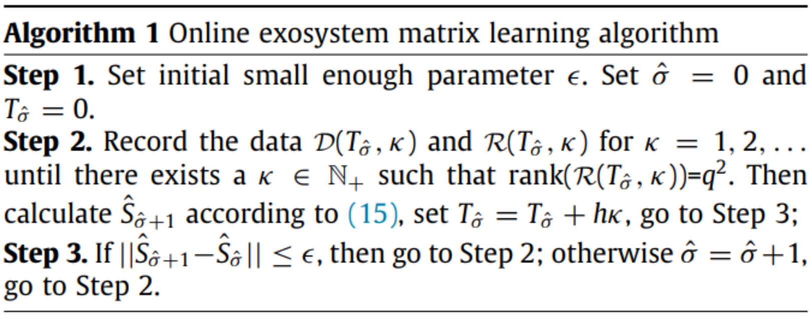


Figure 3.1: Block diagram of closed-loop system.

Previous works on resilient control are only applicable in those cases when the exosystem is time invariant and its dynamics is known to all the agents. An unknown time-varying exosystem model for all agents allows for greater flexibility in many practical situations.

Problem 1. *(Resilient Practical CORP). The heterogeneous MASs (2.1)-(2.2) with unknown switching exosystem dynamics under the influence of DoS attacks are said to achieve resilient practical cooperative output regulation, if for any $\epsilon > 0$ there exist $b_i > 0$ and distributed resilient controllers such that the regulated output $y_i(t)$ is globally ultimately bounded, i.e., $\limsup_{t\to\infty} \|y_i(t)\| \leq b_i\epsilon$ for any initial condition.*

The authors Chao Deng 2022 present a data-driven online learning algorithm to learn the unknown switching exosystem matrix.



Algorithm 1 Online exosystem matrix learning algorithm

Step 1. Set initial small enough parameter ϵ. Set $\hat{\sigma} = 0$ and $T_{\hat{\sigma}} = 0$.

Step 2. Record the data $\mathcal{D}(T_{\hat{\sigma}}, \kappa)$ and $\mathcal{R}(T_{\hat{\sigma}}, \kappa)$ for $\kappa = 1, 2, \ldots$ until there exists a $\kappa \in \mathbb{N}_+$ such that rank($\mathcal{R}(T_{\hat{\sigma}}, \kappa)$)=$q^2$. Then calculate $\hat{S}_{\hat{\sigma}+1}$ according to (15), set $T_{\hat{\sigma}} = T_{\hat{\sigma}} + h\kappa$, go to Step 3;

Step 3. If $||\hat{S}_{\hat{\sigma}+1} - \hat{S}_{\hat{\sigma}}|| \leq \epsilon$, then go to Step 2; otherwise $\hat{\sigma} = \hat{\sigma} + 1$, go to Step 2.

Figure 3.2: Algorithm 1 Online exosystem matrix learning algorithm.

Follows the solution to resilient practical CORP. If distributed observers are designed based on the state of the exosystem directly, then the switching matrix $S_\sigma(t)$ of the exosystem and the matrix $\bar{S}_{\hat{\sigma}}(t)$ of the observers often fall out of synchronization owing to the existence of learning time. In this case, it will be difficult to carry out stability analysis for the resulting closed-loop system. To address this issue, in the first agent, an auxiliary observer $v_0(t)$ is designed to reconstruct the exosystem state $v(t)$ based on the learned exosystem matrix $\bar{S}_{\hat{\sigma}}(t)$.

$$\dot{v}_0(t) = \bar{S}_{\hat{\sigma}} v_0(t) - \aleph_{\hat{\sigma},1}(v_0(t) - v(t)) \tag{3.1}$$

with $\aleph_{\hat{\sigma},1}$ is an observer gain to be determined and $\sigma(t)$ is the switching signal.

Define the reconstruction error as $\tilde{v}_0 = v_0(t) - v(t)$ and $\tilde{S} = S_\sigma - \bar{S}_{\hat{\sigma}}(t)$.

$$\dot{\tilde{v}}_0(t) = (\bar{S}_{\hat{\sigma}} v_0(t) - \aleph_{\hat{\sigma},1} I_q)\tilde{v}_0(t) + \tilde{S} v(t) \tag{3.2}$$

Based on the learning matrix $\bar{S}_{\hat{\sigma}}(t)$, that will be sent to all agents through the communication network, and $v(t)$, the distributed resilient observers $v_i(t)$ will be designed to estimate $v_0(t)$ for each agent even under the influence of DoS attacks. The distributed controller will be designed to achieve the resilient practical cooperative output regulation as follows:

$$\dot{v}_i(t) = \bar{S}_{\hat{\sigma}} v_0(t) - \aleph_{\hat{\sigma},2} \sum_{j=0}^{N} \breve{a}_{ij}(v_i(t) - v_j(t)) \tag{3.3}$$

Based on the solution $(X_{\breve{\sigma},i}(t), U\breve{\sigma}, i(t))$ of the Francis' Equation (2.6) corresponding to the model (2.1), the authors designed the following controller for each agent

$$u_i(t) K_{i,1} x_i(t) + K_{i,2} v_i(t) \tag{3.4}$$

where $K_{i,1}$ is chosen such that the closed loop state matrix is Hurwitz and $K_{i,2} = U\breve{\sigma}, i(t) - K_{i,1} X_{\breve{\sigma},i}(t)$.

The solution of Problem 1 is given by Theorem 1 in [Chao Deng 2022].

3.2 Resilient reinforcement learning and robust output regulation under denial-of-service attacks

In this paper, the authors Jiang 2022 have proposed a novel resilient reinforcement learning approach for solving robust optimal output regulation problems of a class of partially linear systems under both dynamic uncertainties and Denial-of-Service attacks.

The cyber attack is usually unavoidable, therefore, the first problem to address, besides stability and robustness analysis, is how to analyze the resilience of systems against cyber attacks without the knowledge of system dynamics. It is well known that policy iteration (PI) and value iteration (VI) are two typical successive approximation approaches in RL for learning the optimal control policy. Comparing with VI, the convergence of PI is much faster at the price of a strong assumption that an initial admissible control policy must be available. The second problem to discuss is the development of a new successive approximation method that converges quicker than VI and is independent of an initial admissible controller.

The aim of this paper is to solve these two problems in RL based control under denial-of-service (DoS) attacks.

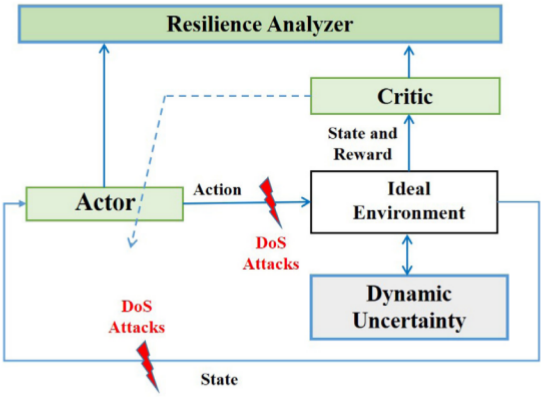
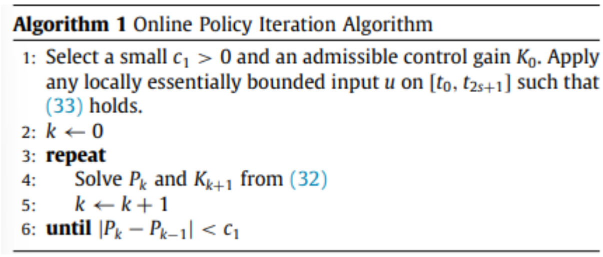


Figure 3.3: The learning framework for the closed-loop system under DoS attacks.

The authors Jiang 2022 will propose three online learning strategies (PI, VI, and HI) to learn the robust optimal control policy $u^* = \tilde{u}^* + Uv := -K_x^* x - K_z^* z$ in terms of online data under the existence of DoS attack (as in Chap.2) during the learning process.

Policy Iteration



```
Algorithm 1 Online Policy Iteration Algorithm
Select a small $c_1 > 0$ and an admissible control gain $K_0$. Apply
  any locally essentially bounded input $u$ on $[t_0, t_{2s+1}]$ such that
  (33) holds.
$k \leftarrow 0$
repeat
    Solve $P_k$ and $K_{k+1}$ from (32)
    $k \leftarrow k + 1$
until $|P_k - P_{k-1}| < c_1$
```

Figure 3.4: Algorithm 1 Online Policy Iteration Algorithm.

In Algorithm 1 in Fig.3.4 the condition that needs to hold comes from the Lemma 2 in [Jiang 2022] and is

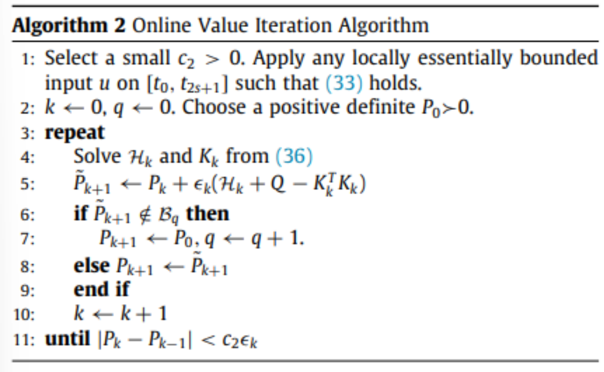
$$rank([\Gamma_{\xi,\xi}, \Gamma_{\xi,\omega}, \Gamma_{\xi,v}]) = \frac{(n+q)(n+3q+3)}{2} \tag{3.5}$$

And computes the policy evaluation $0 = \bar{A}_k^T t P_k + P_k \bar{A}_k + Q + K_k^T K_k$ and the policy improvement $K_{k+1} = \bar{B}^T P_k$, from the linear equation

$$\Psi_{PI}^{(k)} = \begin{bmatrix} vec(P_k) \\ vec(K_{k+1} \\ vec(\bar{D}^T P_k)) \end{bmatrix} = \Phi_{PI}^{(k)} \tag{3.6}$$

with $\bar{A}$ and $\bar{B}$ come from the augmented system defined in [Jiang 2022].

Value Iteration



```
Algorithm 2 Online Value Iteration Algorithm
Select a small $c_2 > 0$. Apply any locally essentially bounded
input $u$ on $[t_0, t_{2s+1}]$ such that (33) holds.
$k \leftarrow 0$, $q \leftarrow 0$. Choose a positive definite $P_0 \succ 0$.
repeat
    Solve $\mathcal{H}_k$ and $K_k$ from (36)
    $\tilde{P}_{k+1} \leftarrow P_k + \epsilon_k(\mathcal{H}_k + Q - K_k^T K_k)$
    if $\tilde{P}_{k+1} \notin \mathcal{B}_q$ then
        $P_{k+1} \leftarrow P_0$, $q \leftarrow q + 1$.
    else $P_{k+1} \leftarrow \tilde{P}_{k+1}$
    end if
    $k \leftarrow k + 1$
until $|P_k - P_{k-1}| < c_2 \epsilon_k$
```

Figure 3.5: Algorithm 2 Online Value Iteration Algorithm.

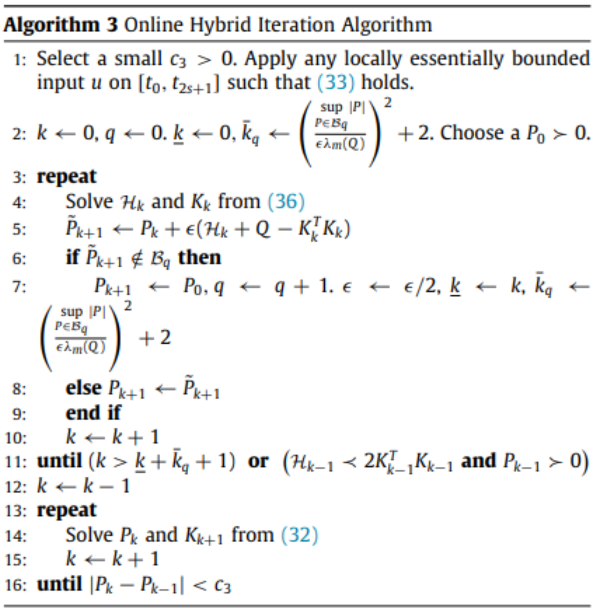
In Algorithm 2 in Fig.3.5 the condition that needs to hold comes from the Lemma 2 in [Jiang 2022] and is the Equation 3.5 and computes $\mathcal{H}_k = \bar{A}_k^T t P_k + P_k \bar{A}_k$ and K_k from

$$\Psi_{PI}^{(k)} = \begin{bmatrix} vec(\mathcal{H}) \\ vec(K_{k+1} \\ vec(\bar{D}^T P_k)) \end{bmatrix} = \Phi_{PI}^{(k)} \tag{3.7}$$

Hybrid Iteration

The VI can be initialized from any initial control policy to learn, but the convergence rate is usually not satisfactory. The PI is a variant of Newton–Raphson method, which can ensure the quadratic convergence but its implementation must rely on an admissible control policy. So that the authors in [Jiang 2022] will propose a new hybrid (HI) algorithm, Algorithm 3 in Fig.3.6, to combine PI and VI efficiently.

In Algorithm 3 in Fig.3.6 the condition that needs to hold comes from the Lemma 2 in [Jiang 2022] and is the Equation 3.5 and computes $\mathcal{H}_k$ and K_k from the Equation 3.7 and also P_k and K_{k+1} from Equation 3.6.



```
Algorithm 3 Online Hybrid Iteration Algorithm
Select a small $c_3 > 0$. Apply any locally essentially bounded input $u$ on $[t_0, t_{2s+1}]$ such that (33) holds.
$k \leftarrow 0$, $q \leftarrow 0$. $\underline{k} \leftarrow 0$, $\bar{k}_q \leftarrow \left(\frac{\sup_{P \in \mathcal{B}_q} |P|}{\epsilon \lambda_m(Q)}\right)^2 + 2$. Choose a $P_0 \succ 0$.
repeat
    Solve $\mathcal{H}_k$ and $K_k$ from (36)
    $\tilde{P}_{k+1} \leftarrow P_k + \epsilon(\mathcal{H}_k + Q - K_k^T K_k)$
    if $\tilde{P}_{k+1} \notin \mathcal{B}_q$ then
        $P_{k+1} \leftarrow P_0$, $q \leftarrow q + 1$. $\epsilon \leftarrow \epsilon/2$, $\underline{k} \leftarrow k$, $\bar{k}_q \leftarrow \left(\frac{\sup_{P \in \mathcal{B}_q} |P|}{\epsilon \lambda_m(Q)}\right)^2 + 2$
    else $P_{k+1} \leftarrow \tilde{P}_{k+1}$
    end if
    $k \leftarrow k + 1$
until $(k > \underline{k} + \bar{k}_q + 1)$ or $\left(\mathcal{H}_{k-1} \prec 2K_{k-1}^T K_{k-1}$ and $P_{k-1} \succ 0\right)$
$k \leftarrow k - 1$
repeat
    Solve $P_k$ and $K_{k+1}$ from (32)
    $k \leftarrow k + 1$
until $|P_k - P_{k-1}| < c_3$
```

Figure 3.6: Algorithm 3 Online Hybrid Iteration Algorithm.

It is shown in Theorem 2 in the article [Jiang 2022] that the Algorithm 3 in Fig.3.6 will always achieve an admissible controller in a finite number of iterations.

3.3 Resilient Output Regulation of Linear Systems Under Denial-of-Service Attacks by Event-Triggered Control

The analyzed article [Yongjie Zhang and Chen 2023] has first discussed the case of DoS attacks on the measurement channel by designing a dynamic output based event-triggered control laws; next, it is developed a class of event-triggered mechanisms in the presence of DoS attacks and finally, the method will be proven by using Lyapunov Analysis. Besides this, the Zeno behaviour (elaborated in Appendix A) can be strictly excluded.

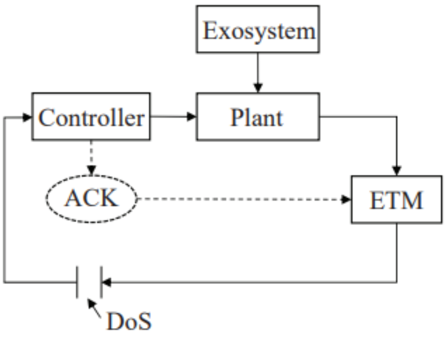


Figure 3.7: Block diagram of the closed-loop system under DoS attacks.

In the Fig.3.7, ETM is an event-triggered mechanism and ACK is an acknowledgement scheme which is used to guarantee that the ETM has knowledge about the reception of packages at the controller side.

Problem 2. *Design a class of event-triggered control laws and a class of event-triggered mechanism, given the plant (2.1) and the exosystem (2.2) in the unreliable network environment with DoS attacks satisfying Assumption 2 and Assumption 3 such that if satisfies*

1. *The trajectory of the closed-loop system is bounded for all* $t \geq 0$*;*
2. *Tracking error* e *converges to an arbitrary small value:* $e \to \varepsilon \quad \text{with } \varepsilon \approx 0$.

Consider a class of event-triggered control law:

$$\begin{cases} u(t) = Kz(t) \\ \dot{z}(t) = \mathcal{G}_1 z(t) + \mathcal{G}_2 e(t_k) \end{cases} \tag{3.8}$$

where

$$\mathcal{G}_1 = \begin{bmatrix} A & E \\ 0 & S \end{bmatrix} + \begin{bmatrix} B \\ 0 \end{bmatrix} K - L\Big(\begin{bmatrix} C & F \end{bmatrix} + DK\Big), \quad \mathcal{G}_2 = L \tag{3.9}$$

$$K = \begin{bmatrix} K_x & K_v \end{bmatrix}, \quad K_v = U - K_x X \tag{3.10}$$

where K_x is a constant matrix such that $\sigma(A + BK_x) \in \mathbb{C}^-$ and L is a constant matrix such that $\sigma(A_L) \in \mathbb{C}^-$ with $A_L = \begin{bmatrix} A & E \\ 0 & S \end{bmatrix} - L \begin{bmatrix} C & F \end{bmatrix}$.

$$e(t_{k+1}) = \begin{cases} e(t_{k+1}), \quad t_{k+1} \in \Theta(t_0, t) \\ e(t_k), \quad t_{k+1} \in \Xi(t_0, t) \end{cases} \tag{3.11}$$

In (3.8), the triggering time instant t_k is generated by the following triggering mechanism:

$$t_{k+1} = \begin{cases} inf\{t > t_k \ni \|\tilde{e}\|^2 \geq \sigma \|e\|^2 + \delta\}, \quad t_k \Theta(t_0, t) \\ r_k + \rho, \quad t_k \in \Xi(t_0, t) \end{cases} \tag{3.12}$$

with σ, ρ and δ are positive real numbers and $\tilde{e}(t) = e(t_k) - e(t)$. Observe that when the network is unreliable then (3.12) grants an approach to decide the next triggering time instant t_{k+1}.

To sum up everything that has been said, let $x_c = col(x, z)$ the closed-loop state vector:

$$\begin{cases} \dot{x}_c = A_c x_c + B_c v + \bar{B}_c \tilde{e} \\ e = C_c x_c + D_c v \end{cases} \tag{3.13}$$

with

$$A_c = \begin{bmatrix} A & BK \\ \mathcal{G}_2 C & \mathcal{G}_1 + \mathcal{G}_2 DK \end{bmatrix} \tag{3.14}$$

$$B_c = \begin{bmatrix} E \\ \mathcal{G}_2 F \end{bmatrix}, \quad \tilde{B}_c = \begin{bmatrix} 0 \\ \mathcal{G}_2 \end{bmatrix}, \quad B_c = \begin{bmatrix} C & DK \end{bmatrix} \tag{3.15}$$

$$D_c = F \tag{3.16}$$

Perform now a change of coordinates on the closed-loop system such that

$$\bar{x}_c = x_c - X_c v \tag{3.17}$$

where X_c satisfies the regulator equation associated to the closed-loop system

$$\begin{aligned} X_c S &= A_c X c + B_c \\ 0 &= C_c X_c + D_c \end{aligned} \tag{3.18}$$

which always exists since Assumption 4 and $\sigma(A_c) \in \mathbb{C}^-$.

Form (3.17) and (3.18):

$$\begin{cases} \dot{\bar{x}}_c = A_c \bar{x}_c + \bar{B}_c \tilde{e} \\ e = C_c \bar{x}_c \end{cases} \tag{3.19}$$

The main result of the authors Yongjie Zhang and Chen 2023 is summarized as the following theorem.

Theorem 1. *Under the assumptions A2 -A7 and the triggering mechanism (3.12), the output regulation problem of the linear system (2.1) and the exosystem (2.2) under DoS attacks can be solved under the control law (3.8), if:*

- $$\sigma < \frac{\phi - 1}{\mu_1} \tag{3.20}$$

with $\phi > 1$ is a positive real number and $\mu_1 := \|P\bar{B}_c C_c\|^2$ and $P > 0$ and symmetric that satisfies $A_c^T P + P A_c = -\phi I$; moreover since A_c is Hurwitz then P always exists.

- $$\frac{\phi}{\tau_{\mathcal{D}}} + \frac{1}{T} < \frac{\omega_1}{\omega_2} \tag{3.21}$$

with ω_1 and ω_2 are some positive numbers.
Furthermore Zeno behaviour is prohibited by formulation of the problem.

In addition to all this, it is important to define, according to the triggering mechanism (3.12) for any $t \in [\, t_k, t_{k+1})$, that when $t_k \in \Theta(t_0, t)$

$$\|\tilde{e}\|^2 \leq \sigma \|e\|^2 + \delta \tag{3.22}$$

which condition holds only in specific intervals characterize as follows.

For any $\tau, t \in \mathbb{R}_{\geq 0}$ with $t \geq \tau \geq 0$, the interval $[\, \tau, t]$ is the disjoint union of $\bar{\Theta}(\tau, t)$ and $\bar{\Xi}(\tau, t)$ where

$$\bar{\Theta}(\tau, t) := \bigcup_{m \in \mathbb{N}_0} Z_m \cap [\, \tau, t] \tag{3.23}$$

$$Z_m := \{p_m\} \cap [\, p_m, p_m + v_m[\tag{3.24}$$

is the union of sub-intervals of $[\, \tau, t]$ where (3.22) holds and $\{p_m\}_{m \in \mathbb{N}_0}$ is a sequence of non-negative and positive real numbers.

$$\bar{\Xi}(\tau, t) := \bigcup_{m \in \mathbb{N}_0} W_{m-1} \cap [\, \tau, t] \tag{3.25}$$

$$W_m := \{p_m + v_m\} \cap [\, p_m + v_m, p_{m+1}[\tag{3.26}$$

is the union of sub-intervals of $[\, \tau, t]$ where (3.22) need no hold, $\{v_m\}_{m \in \mathbb{N}_0}$ is a sequence of non-negative and positive real numbers and $p_{-1} = v_{-1} := 0$.

Chapter 4

Simulations

Follows here a brief discussion of the simulation carried out in the articles [Chao Deng 2022], [Jiang 2022] and [Yongjie Zhang and Chen 2023].

In article [Chao Deng 2022] the MASs considered is composed of 4 mass-spring system. The network topology of the MAS is given in Fig.4.1.

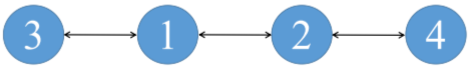


Figure 4.1: The network topology.

In the simulation, only the first agent can receive the information $v(t)$ from the exosystem and so the learning algorithm and the auxiliary observer are equipped in the first agent. The linearised model of each agent is described as (2.1) and (2.2). u_i is the control input (3.4) applied to the agent i. For the values of the matrices of the model, the basis matrices of the exosystem, the switching signal, the observer gains and the initial conditions please refer to the article [Chao Deng 2022].

Case A. In this case the authors Chao Deng 2022 consider DoS attacks.

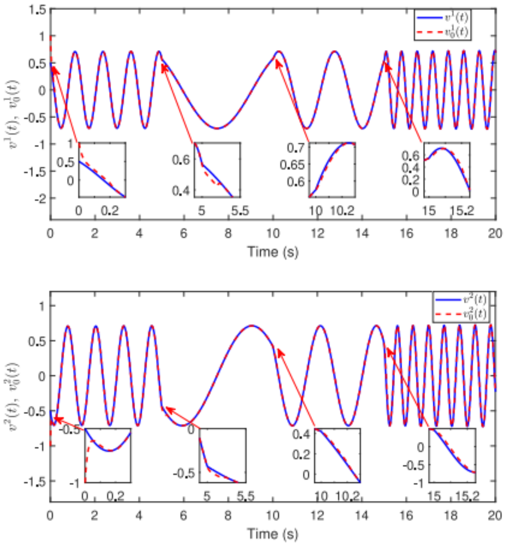


Figure 4.2: Profiles of v^1, v_0^1 (top) and v^2, v_0^2 (bottom) with $\aleph_{\breve{\sigma},1} = 50$.

The trajectories of the exosystem state $v(t) = [v^1(t) \quad v^2(t)]^T$ and the reconstruction state of the auxiliary observer $v_0(t) = [v_0^1(t) \quad v_0^2(t)]^T$ are given in Fig.4.2.

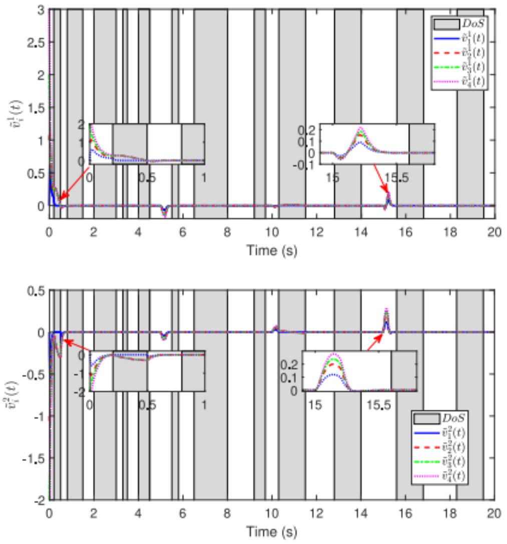


Figure 4.3: Trajectories of the observation errors $\tilde{v}_i^1$, (top) and v_i^2 (bottom) with $\aleph_{\breve{\sigma},2} = 100$.

The trajectories of the resilient observation errors $\tilde{v}_i^1$ and $\tilde{v}_i^2$ which demonstrate that the observation errors are bounded even under the influence of DoS attacks are shown in Fig.4.3.

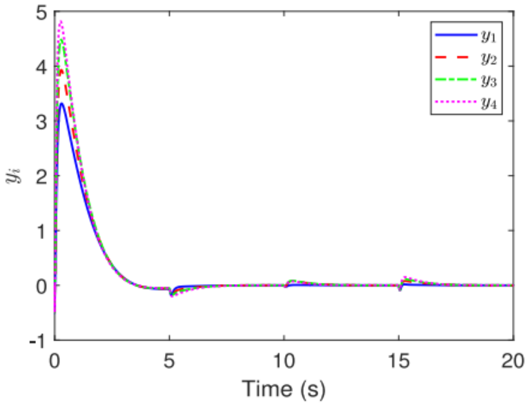


Figure 4.4: Trajectories of regulated output y_i with $\aleph_{\breve{\sigma},1} = 50$ $\aleph_{\breve{\sigma},2} = 100$ in Case A.

The trajectories of the regulated output y_i are displayed in Fig.4.4, which shows that the regulated outputs are bounded in the presence of the DoS attacks.

Case B

To further test and verify the efficiency of our developed method, we compare the above simulation results with the case that $\aleph_{\breve{\sigma},1} = 300$ and $\aleph_{\breve{\sigma},2} = 500$.

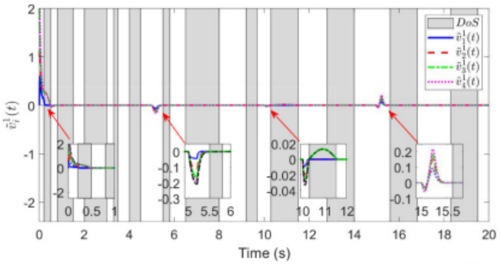


Figure 4.5: Trajectories of the observation errors $\tilde{v}_i^1$ for $i = 1, 2, 3, 4$ with $\aleph_{\breve{\sigma},1} = 50$, $\aleph_{\breve{\sigma},2} = 100$

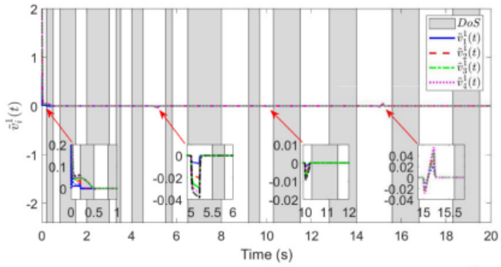


Figure 4.6: Trajectories of the observation errors $\tilde{v}_i^1$ for $i = 1, 2, 3, 4$ with $\aleph_{\breve{\sigma},1} = 300$ $\aleph_{\breve{\sigma},2} = 500$.

In Fig.4.5 and Fig.4.6 the trajectories of the observation errors $\tilde{v}_i^1$ under different observation gains since the trajectories of $\tilde{v}_i^2$ have similar responses.

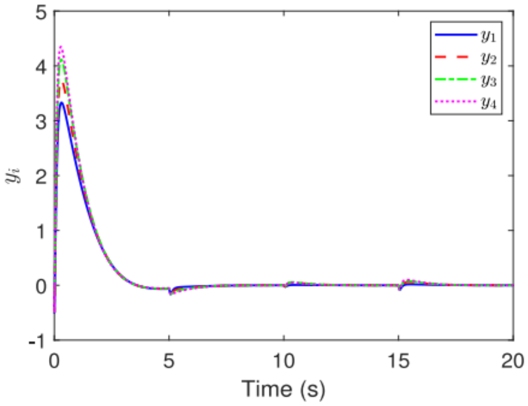


Figure 4.7: Trajectories of regulated output y_i with $\aleph_{\breve{\sigma},1} = 300$ $\aleph_{\breve{\sigma},2} = 500$ in Case B.

In Fig.4.7 the observation errors can be regulated to smaller values by choosing larger observer gains. Besides, trajectories of the regulated output y_i at different values of observation gains.

Case C

In this case it is consider the situation that DoS attacks occur at the switching instant.

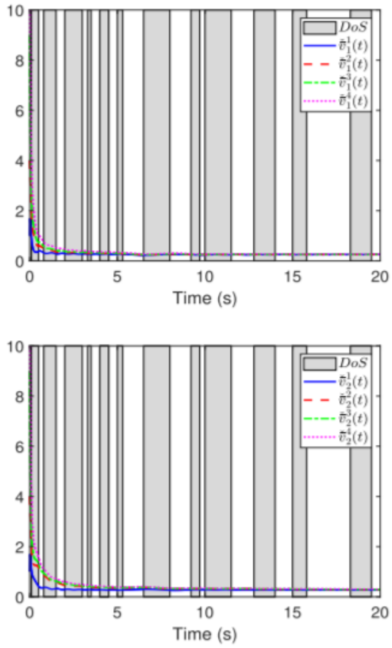


Figure 4.8: Trajectories of mean square errors $\breve{v}_i^1$, (top) and $\breve{v}_i^2$ (bottom).

The DoS attacks and the trajectories of the mean square error $\breve{v}_i^1$ by using the resilient observers (3.2).

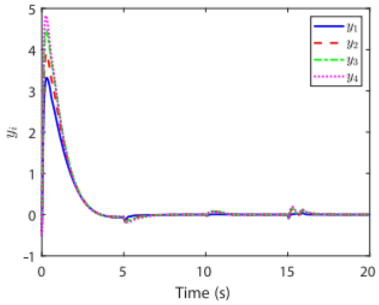


Figure 4.9: Trajectories of regulated output y_i in Case C.

The trajectories of the regulated output y_i are displayed in Fig.4.9.

The authors have observed that more time is required to regulate output $y_i(t)$ when DoS attacks occur at the switching instants in figures from (4.5) to (4.9).

In order to verify the control approach proposed in the article [Jiang 2022], the authors consider, an interconnection of two synchronous generators wherein the generator 2 is regarded as the dynamic uncertainty of generator 1.

Refer to the paper [Jiang 2022] for the values that specify the matrices of the model (2.1) and the exosystem (2.2) and for the values of the constants defined in the HI Algorithm 3 in Fig.3.6.

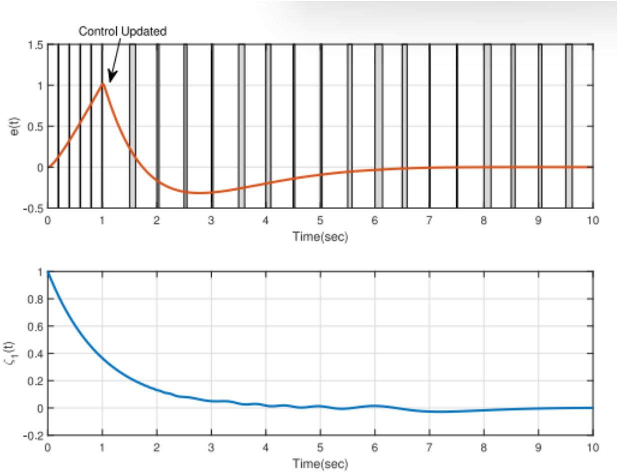


Figure 4.10: The trajectories of angle differences of generator 1 (e) and generator 2 (ζ_1) under DoS attack (shaded areas).

In Fig.4.10 it is possible to see that the DoS duration bound T^* in real life can be much smaller than the theoretic one.

In order to compare the computational complexity of different iteration algorithms, we randomly generate 200 dynamical systems and implement Algorithms in Fig.3.4 to Fig.3.6 to learn the optimal control for each solution.

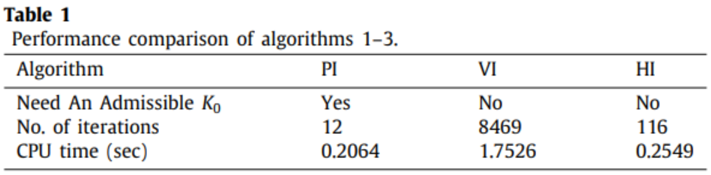


Table 1
Performance comparison of algorithms 1–3.

Algorithm	PI	VI	HI
Need An Admissible K_0	Yes	No	No
No. of iterations	12	8469	116
CPU time (sec)	0.2064	1.7526	0.2549

Figure 4.11: The performance comparison of algorithms VI, PI and HI.

In Fig.4.11 is shown the performance comparison of the algorithms VI (Fig.3.4), PI (Fig.3.5) and the new approach HI (Fig.3.6) on the average CPU time and the number of iterations of each algorithm needed for convergence. It is easy to notice that PI and HI algorithms significantly outperform the VI algorithm, but the PI relies on a strong assumption of an initial stabilizing control gain which is hard to satisfy in real life.

Consider the article [Yongjie Zhang and Chen 2023] and a linear system and a signal v generated by an exosystem of the form considered in Chapter2 where assumptions A4 - A7 are satisfied and design a control law of the form (3.8) which triggering instant is generated by the triggering mechanism (3.12). By taking into account the matrices' values that are reported in the article [Yongjie Zhang and Chen 2023], it is possible to verify that all the eigenvalues of the closed-loop system have negative real part.

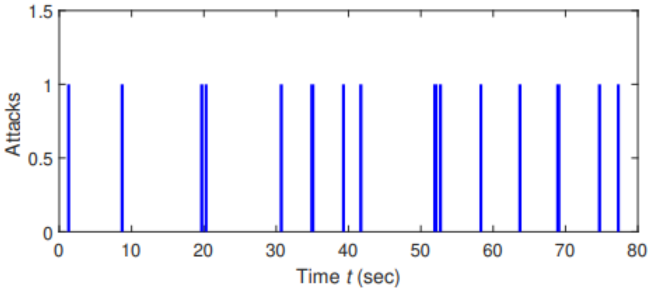


Figure 4.12: Time sequence of DoS attacks.

Let $t_0 = 0$. In Fig.4.12 it has been considered a sequence of fifteen DoS attacks during $t \in [0, 80]$.

Once chosen the parameters of the triggering mechanism and randomly initialised the values of $v(0)$ and $z(0)$ follows the simulation results.

Fig.4.13 shows the evolution of the event triggering condition. Due to DoS attack it is possible to mark the instants of time $t \simeq 2.5\ s$ and $t \simeq 10\ s$ where Equation3.22 is not satisfied.

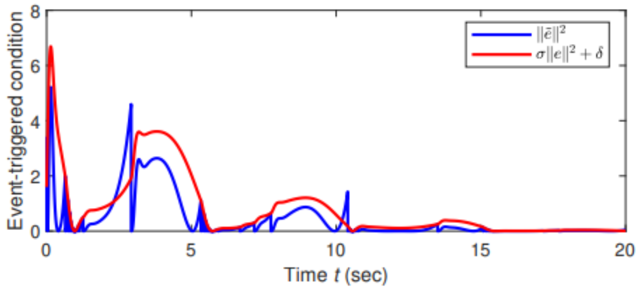


Figure 4.13: Evolution of event-triggered condition.

The Fig.4.14 shows the tracking error of the closed-loop system. It is possible to see that it converges to zero at steady-state.

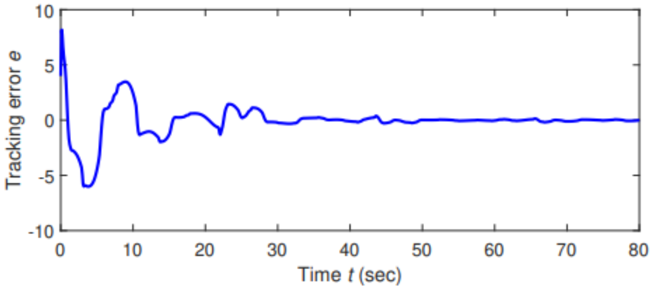


Figure 4.14: Tracking error under DoS attacks.

In general it is possible to observe that the output regulation problem of general linear systems under DoS attacks can be solved by the proposed control law in Chapter3.3.

Chapter 5

Conclusion

Given the increasing vulnerability of the communication network to cyber-attacks it felt interesting to study the works of Chao Deng 2022, Jiang 2022 and, in particular, Yongjie Zhang and Chen 2023. In general the authors of each article presented the resilient output regulation problem of a general linear system (2.1) and (2.2) under DoS attacks by an event-triggered control approach.

In [Chao Deng 2022], it has been investigated the resilient practical CORP for heterogeneous linear MASs with unknown switching exosystem dynamics under DoS attacks. The proposed control scheme consists of a data-driven learning algorithm (Algorithm 1 in Fig.3.2) to learn the unknown switching exosystem matrices, an auxiliary observer to estimate the state of the exosystem (3.2), distributed resilient observers to estimate the state of the auxiliary system (3.3) and distributed controllers (3.4). Moreover, in the paper it has been proved that the observation errors and the regulated errors are globally ultimately bounded.

In [Jiang 2022], it has been studied the reinforcement learning law that assured convergence rate requirement under the challenges from the unknown system and exosystem dynamics. Without relying on the knowledge of system dynamics and initial stabilizing feedback control gain, a new algorithm is proposed, which is capable of learning the optimal regulator using online data with a guaranteed convergence rate (Algorithm 3 in Fig.3.6).

And, last but not least, in [Yongjie Zhang and Chen 2023] it has been first developed a dynamic error output based event-triggered control law (3.8) and an event triggered mechanism (3.12) which can be available under DoS attacks. The resilient output regulation problem is solvable by the control scheme considered and the Zeno behaviour is excluded by construction of the problem.

Finally, I have illustrated the main results of each article through the numerical examples shown in [Chao Deng 2022], [Jiang 2022] and [Yongjie Zhang and Chen 2023] respectively.

Appendix A

Appendix A: Zeno Behaviour

In this section it will be discussed the Zeno behaviour by referring to the article [Sastry 1999].

Given an hybrid system, $H(Q, X, Init, f, Inv, E, G, R)$ where

- Q is a finite collection of discrete variables $\{q_1, q_2, ..\}$,
- $X = \mathbb{R}^n$, $\{x_1, ..., x_n\}$ is a finite collection of continuous states,
- $Init \subseteq Q \times X$ is a set of initial states,
- $f(\cdot, \cdot) : Q \times X \to \mathbb{R}^n$ is a vector field assumed to be Lipschitz,
- $Inv(\cdot) : Q \to 2^X$ assigns to each $q \in Q$ an invariant set,
- $E \subseteq Q \times Q$ is a collection of edges,
- $G(\cdot) : E \to 2^X$ assigns to each edge $e = (q, q') \in E$ a guard,
- $R(\cdot, \cdot) : E \times X \to 2^X$ assigns to each edge $e = (q, q') \in E$ and $x \in X$ a reset relation.

H is called *Zeno* if $\exists (q_0, x_o) \in Init$ such that all infinite executions in $\mathcal{H}^{\infty}_{(q_0, x_0)}$ are Zeno.

An execution is called *Zeno* if it is infinite but the sum of intervals is finite $\sum_i (\tau'_i - \tau_i)$. In other words executions that fail to satisfy conditions of existence and uniqueness of hybrid automata and that show an infinite number of discrete transitions in a finite amount of time are referred to Zeno executions.

Typically the Zeno behaviour arises due to modeling abstractions employed to derive models that are simpler to analyse and control. A way to solve it is by reintroducing some of the physical considerations though the process of regularization which is a standard technique for dealing with differential equations whose solutions are not well defined.

Bibliography

Chao Deng Dan Zhang, Gang Feng (2022). “Resilient practical cooperative output regulation for MASs with unknown switching exosystem dynamics under DoS attacks”. In: *Automatica* 139.

Jiang, Weinan Gao Chao Deng Yi Jiang Zhong-Ping (2022). “Resilient reinforcement learning and robust output regulation under denial-of-service attacks”. In: *Automatica* 142.

Yongjie Zhang Maobin Lu, Fang Deng and Jie Chen (2023). “Resilient Output Regulation of Linear Systems Under Denial-of-Service Attacks by Event-Triggered Control”.

Isidori, Alberto (1995). *Nonlinear Control Systems*. 3rd ed. Springer London.

Dan, Zhang, Deng Chao, and Feng Gang (2023). “Resilient Cooperative Output Regulation for Nonlinear Multiagent Systems Under DoS Attacks”. In: *IEEE Transactions on Automatic Control* 68.4, pp. 2521–2528.

Li, Jun Fu Yiwen Qi Ning Xing Yuzhe (2022). “A new switching law for event-triggered switched systems under DoS attacks”. In: *Automatica* 142.

Michelle S. Chong Henrik Sandberg, André M.H. Teixeira (2019). “A Tutorial Introduction to Security and Privacy for Cyber-Physical Systems”. In: *IEEE* 38, pp. 968–978.

John Lygeros, Shankar Sastry and Claire Tomlin (2020). *Hybrid Systems: Foundations, advanced topics and applications.*

Sutton, Richard S. and Andrew G. Barto (2018). *Reinforcement Learning : an introduction.* ASR.

Sastry, Karl Henrik Johansson Magnus Egerstedt John Lygeros Shankar (1999). “On the regularization of Zeno hybrid automata”. In: *Systems Control Letters* 38, pp. 141–150.