2024 IEEE 63rd Conference on Decision and Control (CDC)
December 16-19, 2024. MiCo, Milan, Italy

A deconvolution-based model predictive control scheme for resilient and maintenance requirements in cyber-physical systems

Domenico Famularo, Giuseppe Franzè and Francesco Tedesco

***Abstract*— In this paper, a constrained regulation problem for networked control systems, whose plants are described by polytopic linear descriptions with a partial state availability, is considered when the communication medium is unreliable. To address the issue, an *ad-hoc* state-estimate control architecture has been deployed via a robust model predictive control strategy that is resilient in achieving regulation goals. Additionally, the proposed scheme is designed to prevent communication disconnections in situations where reaching the origin goal is not viable. A final solid numerical example puts in light the effectiveness and the main benefits of the proposed solution.**

I. INTRODUCTION

In the last years, Cyber-Physical Systems (CPSs) have opened the doors to a myriad of contributions, see e.g., [1]. By now, it is widely accepted that although CPSs play an important role in many practical configurations ranging from manufacturing plants to intelligent transportation systems, see [2] for a comprehensive review, they are quite vulnerable to attacks and interference.

According to this premise, the class of Model Predictive Control (MPC) schemes seems the more adequate approach to formally address resilient issues when constrained CPSs are under malicious intrusions see, e. g., [3]- [5]. Along similar lines are the contributions [6]- [10] where denial-of-service, replay and covert attacks are considered.

Here a novel observer-based resilient MPC control strategy is conceived with a twofold aim: improve the overall control performance by significantly increasing the domain of attraction under which the scheme is capable to contrast long duration false data injection (FDI) occurrences; avoid the use of software rejuvenation procedures [5].

First of all, it is important to underline that the detection phase is different from previous similar approaches. In fact, the possible FDI occurrence is checked both on the plant and control side: the anomaly of the transmitted command input is verified on the plant side, while the corruption of the state measurement on the controller one. Although this prescribes to store a little bit more of data on an actuator buffer, it has the non-trivial advantage to avoid the design of twin model that, by construction, it could reduce the level of data accuracy during the packet transmission along the *sensor-to-controller* and *controller-to-actuator* channels. Hence under the initial assumption that the plant is attack-free, the system is regulated by resorting to a control strategy, hereafter denotes as **Healthy-MPC**, designed according to the prescriptions of [16] with a single time instant delay. In order to make viable this approach, the domain of attraction of the **Healthy-MPC** must be made safe, this is achieved by proceeding along two parallel ways: 1) define a resilient control strategy **Resilient-MPC** whose domain of attraction is a subset of the **Healthy-MPC** one and where a MPC sequence of length N is *ad-hoc* designed to drive the system within a robust positively invariant region centered at the origin; 2) off-line individuate a set of so-called *parking spots* where the plant can lie until the attack ends. This prescribes to determine a set of controllers, named **Maintenance-MPC**, centered at the *parking spots* such that the resulting domain of attractions plus the **Resilient-MPC** region completely cover the **Healthy-MPC** one. Notice that such an approach is in charge to support real time updates by keeping alive the system thanks the action of another controller until the normal operations are restarted [17]. Broadly speaking, in the present approach and unlike from the standard literature meaning, the maintenance operations are in charge to allow the plant of reducing as much as possible the failure probability: this is done by off-line identifying a set of safe and admissible dynamical behaviors that the regulated plant can "track", even in a *stand-by* mode, until the operating conditions go back to being favorable for satisfying the prescribed goal.

This work was supported by the research project - ID:20222N4C8E "Resilient and Secure Networked Multivehicle Systems in Adversary Environments" granted by the Italian Ministry of University and Research (MUR) within the PRIN 2022 program.

Giuseppe Franzè is with DIMEG - Università della Calabria, Via Pietro Bucci, 44-C, Rende (CS), 87036, ITALY, {giuseppe.franze}@unical.it

Domenico Famularo and Francesco Tedesco are with DIMES - Università della Calabria, Via Pietro Bucci, 42-C, Rende (CS), 87036, ITALY, {domenico.famularo,francesco.tedesco}@unical.it

NOTATION

Consider the discrete time linear model

$$x(t+1) = A\,x(t) + B_u\,u(t) + B_d\,d(t) \tag{1}$$

where $t \in \mathbb{Z}_+ := \{0, 1, ...\}$, $x(t) \in \mathbb{R}^{n_x}$, $u(t) \in \mathbb{R}^{n_u}$, $d(t) \in \mathbb{R}^{n_d}$ and

$$\left[\begin{array}{ccc} A & B_u & B_d \end{array}\right] \in \mathbf{co}\left(\left\{\left[\begin{array}{ccc} A_i & B_{u,i} & B_{d,i} \end{array}\right]\right\}_{i=1}^{n_p}\right) \tag{2}$$

with $\mathbf{co}(\cdot)$ the convex-hull operator, the one-step-ahead map is then a set of states which, for a given triplet $\{x,\ u,\ d\}$, $x \in \mathbb{R}^{n_x}$, $u \in \mathbb{R}^{n_u}$, $d \in \mathbb{R}^{n_d}$, is characterized as follows

$$\begin{array}{l} \mathscr{X}\left([A,\ B_u,\ B_d],\ \{x,\ u,\ d\}\right) := \\ \left\{\xi \in \mathbb{R}^{n_x} \mid \xi = \sum_{i=1}^{n_p} \alpha_i A_i\,x + \sum_{i=1}^{n_p} \alpha_i B_{u,i}\,u + \right. \\ \left. + \sum_{i=1}^{n_p} \alpha_i B_{d,i}\,d,\ \alpha_i \geq 0,\ i = 1, \ldots, n_p \quad \sum_{i=1}^{n_p} \alpha_i = 1\right\} \end{array}$$

the k-th steps ahead map

$$\mathscr{X}^k\left([A,\ B_u,\ B_d],\ \left\{x,\ \{u(i)\}_{i=0}^{k-1},\ \{d(i)\}_{i=0}^{k-1}\right\}\right), k \geq 1$$

is recursively defined as

$$\begin{cases} \mathscr{X}^1\left([A,\ B_u,\ B_d],\ \{x,\ u(0),\ d(0)\}\right) := \\ \qquad \mathscr{X}\left([A,\ B_u,\ B_d],\ \{x,\ u(0),\ d(0)\}\right) \\ \mathscr{X}^k\left([A,\ B_u,\ B_d],\ \left\{x,\ \{u(i)\}_{i=0}^{k-1},\ \{d(i)\}_{i=0}^{k-1}\right\}\right) := \\ \qquad \mathscr{X}\left([A,\ B_u,\ B_d],\ \left\{\mathscr{X}^{k-1}\left([A,\ B_u,\ B_d]\right.\right.\right. \\ \left.\left.\left.\left\{x,\ \{u(i)\}_{i=0}^{k-2},\ \{d(i)\}_{i=0}^{k-2}\right\}\right),\ u(k-1),\ d(k-1)\right\}\right), \\ \qquad k>1 \end{cases}$$

Let $v(t+k|t) \triangleq v_k(t) = \hat{v}_k$ be the $k-$steps state ahead prediction of a generic system variable v from t onward.
Given a sequence of vector $W = \{w_1, \ldots, w_l\}$, $w_i \in \mathbb{R}^{n_w}$, $dim(W)$ denotes its length.
The vector 0_n denote the column vector of n zero entries, while I_n is the $n \times n$ identity matrix.

II. Problem formulation

Consider the class of systems described by the following polytopic state space models

$$\begin{cases} x(t+1) &= Ax(t) + Bu(t) + d(t) \\ y^s(t) &= C\,x(t) + v(t) \end{cases} \tag{3}$$

where $x(t) \in \mathbb{R}^{n_x}$ denotes the state, $u(t) \in \mathbb{R}^{n_u}$ the command input, $d(t) \in \mathbb{R}^{n_d}$ an exogenous disturbance, $y^s(t) \in \mathbb{R}^{n_y}$ the measured output and $v(t) \in \mathbb{R}^{n_v}$ the sensor error measurement,

$$\left[\begin{array}{cc} A & B \end{array}\right] \in \mathbf{co}\left(\left\{\left[\begin{array}{cc} A_i & B_i \end{array}\right]\right\}_{i=1}^{n_p}\right) \tag{4}$$

and the measurement matrix $C \in \mathbb{R}^{n_y \times n_u}$ is known. Moreover, the following state and input constraints are prescribed:

$$\begin{array}{l} u(t) \in \mathcal{U} := \{u \in \mathbb{R}^{n_u} : u^T u \le u_{max}^2\}, \\ x(t) \in \mathcal{X} := \{x \in \mathbb{R}^{n_x} : x^T x \le x_{max}^2\},\ \forall t \ge 0, \end{array} \tag{5}$$

with $\mathcal{U}$ and $\mathcal{X}$ compact subsets of $\mathbb{R}^{n_u}$ and $\mathbb{R}^{n_x}$, respectively, and $0_{n_u} \in \mathcal{U}$, $0_{n_x} \in \mathcal{X}$. Moreover the exogenous disturbance and the error measurement are persistent but bounded signals $d(t) \in \mathcal{D} := \{d \in \mathbb{R}^{n_x} | d^T d \le \bar{d}\} \subset \mathbb{R}^{n_x}$ and $v(t) \in \mathcal{V} := \{v \in \mathbb{R}^{n_y} | v^T v \le \bar{v}\} \subset \mathbb{R}^{n_y}$, respectively.
Physical plant operations are supported by a communication network where sensor measurements and command data are transmitted and, since the communication network may be unreliable, the data exchanged between the controller and the plant may be possibly corrupted by malicious cyber-attacks so that $u(t) \neq u^a(t)$ and $y(t) \neq y^s(t)$ for some $t \in \mathbb{Z}$. i.e. $u(t) \in \mathbb{R}^{n_u}$ and $y(t) \in \mathbb{R}^{n_y}$ may denote corrupted control signals and output measurements, respectively.
Then, the problem to solve is stated as follows:

Output resilient control for Cyber-Physical Systems (ORC-CPS) - *Given the plant (3), subject to the constraints (5), design, under the occurrence of FDI attacks on both communication channels:*

- *a detection framework capable to reveal unfavorable and/or malicious events;*
- *a feedback control law on the basis of the available measurements* $u(t) = g(\{y^s(t),\ y^s(t-1),\ \ldots\})$ *such that, despite any admissible disturbance/noise realization, the regulated augmented plant trajectory is minimum variance and uniformly ultimate bounded [13].*

III. Proposed solution outline

The state estimation question is here approached by deconvolution filtering arguments [14] where the state observer is

$$x_F(t+1) = A_F\,x_F(t) + B_{F_y}\,y(t) + B_{F_u}\,u(t) \tag{6}$$

with $x_F(t) \in \mathbb{R}^{n_x}$ denoting the state plant estimate. As consequence, the estimation error

$$e(t) \triangleq x(t) - x_F(t) \tag{7}$$

characterizes the discrepancy between the state and its estimate and the initial value, $e(0)$, is assumed to belong to the following ellipsoidal set

$$\mathcal{H} \triangleq \{e \in \mathbb{R}^{n_x} \,|\, e^T\,\Psi_H\,e \le 1\} \tag{8}$$

where $\Psi_H = \Psi_H^T > 0$, $\Psi_H \in \mathbb{R}^{n_x \times n_x}$ denotes the initial *confidence* shaping matrix for the state estimation error. Therefore, from now on the closed-loop system is described in terms of the augmented state $s^T(t) \triangleq [x_F^T(t)\ \ e^T(t)]^T \in \mathbb{R}^{2\,n_x}$. The second premise concerns with the system liveness when unpredictable external intrusions prevent and/or deteriorate the normal system operations. To this end, the idea consists in introducing two operating settings (**OP**): **Normal OP** : the zero *disturbance free* nominal equilibrium triplet $(x_0^e,\ u_0^e,\ y_0^{s,e}) \equiv \left(0_{n_x},\ 0_{n_u},\ 0_{n_y}\right)$ which represents a *satisfactory* time behavior; **Maintenance OP** : a finite collection of $i = 1,\ 2,\ \ldots,\ L > 0$ equilibrium points (i.e. *parking spots*) belonging to the plant operating region $(x_i^e,\ u_i^e,\ y_i^{s,e}) \neq \left(0_{n_x},\ 0_{n_u},\ 0_{n_y}\right)$, i.e. safe although not satisfactory plant configuration.
The reasons behind this characterization can be better understood according to the following reasoning. Three different scenarios are considered: 1) healthy operations: in absence of unfavorable events one has the domain of attraction (DoA) $\mathcal{T}$ associated to the stabilizing control law $g_{\mathcal{T}}(x)$; 2) resilient operations: the region Ω, associated to $g_\Omega(x)$, collects all the plant states for which there exists a sequence of admissible commands capable to accomplish the prescribed task despite FDI occurrences; 3) maintenance operations: the pairs $(\Theta_i, g_{\Theta_i}(x))$, $i = 1, \ldots, L$, designed with respect to the equilibria $x_i^e, i = 1, \ldots, L$, for which during malicious intrusions there exists a sequence of admissible commands capable to drive the regulated plant trajectory towards a safe neighbor of x_i^e. It is important to underline that the DoAs Θ_i are overlapped because they are computed under the fulfillment of the following set-inclusion

$$\mathcal{T} \setminus \Omega \subseteq \bigcup_{i=1}^{L} \Theta^i \tag{9}$$

As the FDI occurrence is concerned, it is assumed that *a-priori* information are not available and any delivered data along the communication medium could be affected. Then, the proposed control architecture is schematically reported in Fig. 1. There, at each time instant the deconvolution filter (6) receives the state measurement $y(t)$ exploited together

with the computed control action $\bar{u}(t)$ for state estimation purposes, i.e., $x_F(t)$. The *Controller* is designed by resorting

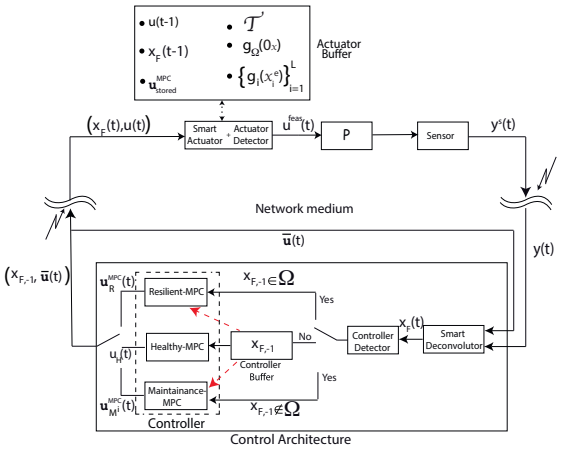

Fig. 1. An estimator based *maintenance devoted* control architecture against FDI attacks

to well-established MPC ideas here properly adapted to the state estimate case. According to the above discussion, three observer based control units are considered: **Healthy-MPC** used in attack-free scenarios and in charge to regulate the plant towards the **Normal OP**; **Resilient-MPC** usable when the attack is underway and the state estimate belongs to its DoA, i.e., $x_F(t) \in \Omega$; by construction it asymptotically drives the regulated state trajectory towards the **Normal OP**; **Maintenance-MPC** usable when the plant is recognized to be under attack and the state estimation is outside Ω, i.e. $x_F(t) \in \Theta^i$. It drives the state trajectory towards a neighbor of the *parking spot* x_i^e (**Maintenance OP**) and there it is confined until a recovery phase takes place.

The *Controller Buffer* is introduced to store the last attack-free state estimate $x_{F,-1}$ to be used, whenever necessary, to update the controllers **Resilient-MPC** and **Maintenance-MPC** and to be shared with the plant side for detection purposes. Since the controller output $\bar{u}(t)$ strictly depends on the attack scenario, it can be a single action $u_H(t)$ or a sequence of commands $(\mathbf{u}_R^{MPC}(t), \mathbf{u}_{M_i}^{MPC}(t))$ that are timely and properly exploited by the **Deconvolutor**.

On the plant side, it is assumed that an *Actuator Buffer* takes trace of the following data: 1) the command $u(t-1)$ related to the attack-free scenario that is feasible at the current time instant t; 2) the healthy domain of attraction $\mathcal{T}$ and its state-dependent control law $g_{\mathcal{T}}(x)$; 3) a sequence of admissible commands $\mathbf{u}_{stored}^{MPC}$ selected within the family $\left\{\mathbf{u}_R^{MPC}(t) \cup \left\{\mathbf{u}_{M_i}^{MPC}(t)\right\}_{i=1}^{L}\right\}$; 4) the state-dependent control laws $g_\Omega(x)$ and $g_{\Theta_i}(x)$ associated to the regions Ω and Θ^i, $i = 1, \ldots, L$.

Moreover, a **Smart Actuator** is in charge to recognize the structure of the received packet $(x_F(t), u(t), \mathbf{u}_{current}^{MPC}(t))$ and to perform adequate actions:

- $u(t)$ is a single command: the **Actuator Buffer** is activated and, by using x_F and the healthy DoA ($\mathcal{T}$), anomalous behaviors are investigated. If an attack is underway, $u_{feas}(t) \leftarrow u(t-1)$ otherwise $u_{feas}(t) \leftarrow u(t)$ and $u(t-1) \leftarrow u(t)$ and $\mathbf{u}_{stored}^{MPC} \leftarrow \mathbf{u}_{current}^{MPC}(t)$;
- $u(t)$ is the sequence $\mathbf{u}_R^{MPC}(t)$: the plant is under attack and $x_{F,-1} \in \Omega$. Then, $u_{feas}(t) \leftarrow \mathbf{u}_{stored,k}^{MPC}$ is $k-th$ move;
- $u(t)$ is the sequence $\mathbf{u}_{M^i}^{MPC}(t)$: the plant is under attack and $x_{F,-1} \in \Theta^i$. Then, $u_{feas}(t) \leftarrow \mathbf{u}_{stored,k}^{MPC}$ is $k-th$ move.

Once the attack has been revealed, the plant proceeds in an open-loop fashion according to the sequence $\mathbf{u}_{stored}^{MPC}$ towards 0_x (resp. x_i^e) the state trajectory can be indefinitely confined within a neighbor of 0_x (resp. x_i^e) under the action of $g_\Omega(0_x)$ ($g_{\Theta^i}(x_i^e)$). Notice that the resilient controller leads to the satisfaction of the **ORC-CPS**, while $\mathbf{u}_{M^i}^{MPC}(t)$ drives the plant to the parking spot x_i^e where it remains in a *Maintenance OP* mode thanks to $g_{\Theta^i}(x_i^e)$ until a recovery phase is completed. Then, a switching to the **Healthy-MPC** comes to play and the above procedure is iterated.

Finally, it is important to underline that $\mathbf{u}_{stored}^{MPC}$ is updated whenever an attack is detected and the **Resilient-MPC** ($x_{F,-1} \in \Omega$)) or a **Maintenance-MPC** ($x_{F,-1} \notin \Omega \wedge x_{F,-1} \in \Theta^i$) scheme should be applied. Since the *controller-to-actuator* link is always unreliable, it is required that the following operating assumption must hold.

Assumption 1 *After any anomaly detection, a data protection mechanism along the controller-to-actuator channel is adopted so that, for at least a time instant, inferences on the packet integrity are hampered.* □

IV. The Resilient and Maintenance Receding Horizon Control Architecture

In the sequel, the set-theoretic receding horizon control strategy [12] is customized to the architecture of Fig. 1.

A. Controller

1) Healthy-MPC: The **Healthy-MPC** unit is designed under the following reasoning. Since this controller acts during the on-line normal operations, the packet $(x_{F,-1}, \bar{\mathbf{u}})$ could be affected during the transmission along the controller-to-actuator channel and the anomaly detected directly on the plant side (via the **Actuator Detector**), it must be ensured that an admissible command is always available to be applied before the switching to the **Resilient-MPC** or **Maintenance-MPC** units is viable. Therefore, the idea is to design **Healthy-MPC** such any its control action is feasible for two consecutive time instant. To this end, the arguments of [16] are customized to the proposed framework.

First, an admissible terminal region is derived by considering the following state-feedback control law

$$u_H(t) = K_H\, x_F(t-1) \tag{10}$$

which satisfies the prescribed constraints (5) and ensures that the regulated state trajectory

$$s(t+1) \in \mathscr{X}\left([\Phi,\ \Upsilon,\ \Gamma],\ \left\{s(t),\ u_H(t), \begin{bmatrix} d(t) \\ v(t) \end{bmatrix}\right\}\right) \tag{11}$$

where

$$\Phi := \begin{bmatrix} A_F + B_{F_y} C & B_{F_y} C \\ A - A_F - B_{F_y} C & A - B_{F_y} C \end{bmatrix}, \ \Upsilon := \begin{bmatrix} B_{F_u} \\ B - B_{F_u} \end{bmatrix},$$

$$\Gamma := \begin{bmatrix} 0 & B_{F_y} \\ I & -B_{F_y} \end{bmatrix}$$

enjoys minimum variance irrespective of the delay occurrence $\tau(t) \leq 1$ and $\forall \alpha \in \Sigma$, $\forall n(t) \in \mathcal{N}$, $\forall d(t) \in \mathcal{D}$. By resorting to standard technicalities in time-delay systems, [15], the following description is obtained from (11)

$$\begin{cases} s(t+1) &= h(t) + s(t) \\ 0 &= -h(t) + \Phi\, s(t) - s(t) + \Upsilon\, K_H\, x_F(t-1) + \\ & \quad \Gamma \begin{bmatrix} d(t) \\ v(t) \end{bmatrix} \end{cases} \tag{12}$$

where $h(t) := s(t+1) - s(t)$. By defining the augmented state $\bar{s}(t) = \left[s^T(t)\ h^T(t)\right]^T \in \mathbb{R}^{4\,n_x}$, it can be proven that the ellipsoidal set

$$\mathcal{E} \triangleq \mathrm{Proj}_{x_F}\{\bar{s} \in \mathbb{R}^{4\,n_x} \mid \ \bar{s}^T \Psi_{\bar{s}} \bar{s} \leq 1\}$$

is a robust positively invariant region [13] for the closed-loop state evolutions (11) complying with state and input constraints (5), i.e $\mathcal{E} \subset \mathcal{X}$ and $K_H \mathcal{E} \subset \mathcal{U}$ irrespective of the one-time delay occurrence, estimation error $e(t) \in \mathcal{H}$ and any noise/disturbance realizations $n(t) \in \mathcal{V}$ and $d(t) \in \mathcal{D}$.
Hence, the sequence the ellipsoidal approximations of the one-step state ahead controllable sets for the DT-LDI (3), hereafter denoted as $\{\mathcal{E}_i\}$, are computed by resorting to the arguments developed in [16].

Finally, given a generic state estimate x_F the Healthy-MPC module updates the control move $u_H(t)$ according to the following optimization problem

$$u_H(t) := \quad \arg\min F_{j(t)}(x_F, u_H) \ \text{ s.t.} \tag{13}$$

$$\mathrm{Proj}_{x_F}\mathscr{X}\left([\Phi,\ \Upsilon],\ \{s,\ u_H\}\right) \in \mathcal{E}_{i(t)-1}, \alpha \in \Sigma \tag{14}$$

where $F_{j(t)}(x_F, u_H) \in \mathbf{F} := \{F_h(x_F, u_H)\}_{h=1}^{r}$ is a set of penalizing functions that are randomly chosen at each time instant by the real-valued function $j(t) : \mathbb{Z}_+ \to \{1, \ldots, r\}$.

2) Resilient-MPC: The **Resilient-MPC** unit is designed under the following prescriptions. Whenever an attack has been detected and the current state estimate $x_F \in \Omega$, the control mode switching **Healthy-MPC** $\rightarrow$ **Resilient-MPC** takes place, the resulting regulated state trajectory is driven in a finite number of steps, say N, to a neighborhood of 0_{n_x} and there indefinitely confined. To comply with these requirements, the **Resilient-MPC** is hereafter designed as a MPC controller of length N according to the following requirements: 1) the domain of attraction of **Resilient-MPC** is strictly contained in that of the **Healthy-MPC**; 2) $\mathbf{u}_R^{MPC}(t) \triangleq \{u_H(t-1), \hat{u}_{R,1}^{MPC} \ldots, \hat{u}_{R,N-1}^{MPC}\}$.
The point 2) is mandatory to harmonize the resilience action with the healthy mode when the attack is detected by the **Actuator Buffer** and the previous computed command $u_H(t-1)$ has been applied.
Let $N \leq \bar{N}_R$, with $\bar{N}_R$ the upper bound on the control horizon length, and $x_F \in \Xi_i^N$ be given, then the following convex optimization problem is stated:

$$\min_{\{\hat{u}_{R,k}^{MPC}\}} \ J(x_F, \mathbf{u}_R^{MPC}) \tag{15}$$

$$\hat{x}_{F,\,k+1} \in \mathrm{Proj}_{x_F}\mathscr{X}\left([\Phi,\ \Upsilon,\ \Gamma],\ \left\{s_k, \hat{u}_{R,k}^{MPC},\ \left[d_k^T,\ v_k^T\right]\right\}\right) \quad \forall d_k \in \mathcal{D},\ v_k \in \mathcal{V},\ e_k \in \mathcal{H} \tag{16}$$

$$\hat{x}_{F,0} = A_F x_{F,-1} + B_{F_y} y(t-1) + B_{F_u} u_H(t-1) \tag{17}$$

$$\hat{u}_{R,k}^{MPC} \in \mathcal{U},\ k = 1, \ldots, N-1; \tag{18}$$

$$\hat{x}_{F,k} \in \Xi_{N-k}, k = 2, \ldots, N-1; \tag{19}$$

$$\hat{x}_{F,N} \in \Xi_0; \tag{20}$$

where

$$J(x_F, \mathbf{u}_R^{MPC}) \triangleq \min_{u_{R,k}^{MPC}} \sum_{k=0}^{N-1} \left[\|\hat{x}_{F,k}\|_{R_{x_F}}^2 + \|u_{R,k}^{MPC}\|_{R_u}^2\right] \tag{21}$$

with $R_{x_F} = R_{x_F}^T \geq 0$ and $R_u = R_u^T > 0$ state and input shaping matrices, respectively.

3) Maintenance-MPC: Here, the aim is to design a bank of **Maintenance-MPC** units such the associated domains of attraction Θ^i, $i = 1, \ldots, L$, comply with the requirement (9). This is instrumental to take care of attack scenarios when $x_{F,-1} \notin \Omega$ and $x_{F,-1} \in \Theta^i$, and the control mode switching is mandatory **Healthy-MPC** $\rightarrow$ **Maintainance-MPC**. In such a case, the resulting regulated state trajectory is driven in a finite number of steps to a neighborhood of x_i^e and there is confined until a recovery phase is completed. The idea is to determine a sequence of MPC controllers $\mathbf{u}_{M_i}^{MPC}(t) \triangleq \{u_H(t-1), \ldots, \hat{u}_{M^i,N-1}^{MPC}\}, i = 1, \ldots, L$, such the associated domains of attraction Θ^i, $i = 1, \ldots, L$, comply with the requirement (9). Similar arguments of the **Resilient-MPC** section are exploited with (x_i^e, u_i^e) in place of $(0_x, 0_u)$.
Let $\Theta_0^i, i = 1, \ldots, L$, be the RPI region centered at x_i^e and K_{M^i} the associated stabilizing state estimate feedback laws, then the sequence of time-delay free one-step state ahead controllable sets is given by the following recursions:

$$\begin{aligned} \Theta_j^i \ := \mathrm{Proj}_{x_F}\Bigg\{ s : \exists u \in \mathcal{U} \ \mid \ \mathrm{Proj}_{x_F}\mathscr{X}\Big([\Phi,\ \Upsilon,\ \Gamma], \\ \left\{s,\ u,\ \left[d^T,\ v^T\right]^T\right\}\Big) \in \Theta_i^{j-1},\ x_F \in \mathcal{X} \\ \forall e \in \mathcal{H}, \forall d \in \mathcal{D}, \forall v \in \mathcal{V} \Bigg\}, i = 1, \ldots, L \end{aligned}$$

As outlined in the previous section, the computation of the sequence of moves $\mathbf{u}_{M_i}^{MPC}$ prescribes to take care of the $k-step$ ahead state predictions

$$\hat{s}_k \in \mathscr{X}^k\left([\Phi, \Upsilon, \Gamma], \left\{\hat{s}_0, \left\{\hat{u}_{M^i,j}^{MPC}\right\}_{j=0}^{k}, \left\{\left[d_j^T, v_j^T\right]^T\right\}_{j=0}^{k}\right\}\right)$$
$$k = 0, \ldots, N-1$$

Then, in order to ensure the recursive feasibility property, the family $\{\Theta_j^i\}$ must redefined by taking into account the

disturbance component

$$\mathscr{X}^k\left([\Phi,\Upsilon,\Gamma],\left\{0_{2\,n_x},\ \{0_{n_u}\}_{j=0}^{k},\left\{\left[d_j^T,v_j^T\right]^T\right\}_{j=0}^{k}\right\}\right)$$

Therefore, one has:

$$\begin{aligned}\Pi_0^i = &\ \Theta_i^0\\ \Pi_j^i = &\ \mathrm{Proj}_{x_F}\Bigg\{s\in\mathbb{R}^{2\,n_x}:\exists u\\ &\ \left|\mathscr{X}\Big([\Phi,\Upsilon,\Gamma],\left\{s,\ u,\left[\begin{array}{c}d\\v\end{array}\right]\right\}\Big)\subseteq\tilde{\Theta}_{j-1}^i\right\}\end{aligned}$$

where

$$\begin{aligned}&\tilde{\Theta}_j^i:=\Theta_i^j\sim\mathrm{Proj}_{x_F}\Bigg\{s\in\mathbb{R}^{2\,n_x}:\mathscr{X}^{N-j-1}\Big([\Phi,\ \Upsilon,\ \Gamma],\\ &\left(\left[\begin{array}{c}x_i^e\\0_{n_x}\end{array}\right],\ \{u_i^e\}_{k=0}^{N-j-1},\ \left\{\left[\begin{array}{c}d_k\\v_k\end{array}\right]\right\}_{k=0}^{N-j-1}\right)\Big)\subseteq\tilde{\Theta}_{N-j-1}^i\Bigg\},\\ &j=1,\ldots,N-1\end{aligned}$$

Then by assuming that $x_F\in\Pi_N^i$ the same convex optimization (15)-(20), with $J(x_F-x_i^e,\tilde{u}-u_i^e)$ in place of (21) and $\{\Pi_j^i\}$ in place of $\{\Xi_j\}$, comes out.

B. Detector units

As shown in Fig. 1, this task is split in two phases and the **Actuator Buffer** stores the sequence of healthy one-step state ahead controllable sets in the extended space $(\bar{\chi},u_H)$, i.e., $\{\mathcal{T}_i^{ext}\}_{i=1}^N$, i.e., the domain of attraction $\mathcal{T}:=\bigcup_{i=1}^{N}\mathcal{T}_i^{ext}$.

Actuator Detector -

On the plant side, it is checked if the command input $\bar{\mathbf{u}}(t)$ is altered by the action of the malicious agent via a FDI $u^a(t)$. This can be done by resorting to set-membership arguments by defining the prediction set:

$$\begin{aligned}&\mathbf{U}^+\left(x_F(t-1),\ u(t-1)\right):=\\ &\Big\{[x_F^T\ u^T]\in\mathbb{R}^{n_x+n_u}\,|\,[x_F^T\ u^T]^T\in\mathrm{Proj}_{x_F,u}\mathscr{X}\left([\Phi,\ \Upsilon,\ \Gamma],\right.\\ &\left.\left\{\left[x_F(t-1)^T,\ e^T\right]^T,u(t-1),\ \left[d^T,\ v^T\right]\right\}\right),\\ &\left.\forall d\in\mathcal{D},\ v\in\mathcal{V},\ e\in\mathcal{H}\right\}\subset\mathrm{Proj}_{x_F,u}\mathcal{T}_{i-1}^{ext}\end{aligned}$$

Then, the following detection logic comes out

$$\mathbf{D}_U^+(x_F(t),u(t)):=\begin{cases}\text{attack}, & \text{if } [x_F(t)^T,u(t)^T]^T\notin\\ & \mathbf{U}^+\left(x_F(t-1),u(t-1)\right)\\ \text{no attack}, & \text{otherwise}\end{cases}$$

Controller Detector -

The validity of the received output measurement $y(t)$ is checked from the application of the feasible command $u_{H,-1}(t)$ and the estimate based attack-free measurement $x_{F,-1}$ stored in the **Controller Buffer**. Specifically, the prediction set $\mathbf{Z}^+$ is:

$$\begin{aligned}&\mathbf{Z}^+\left(x_{F,-1},u_{H,-1}\right):=\Big\{x_F^+\in\mathbb{R}^{n_x}|x_F^+\in\mathrm{Proj}_{x_F}\mathscr{X}\left([\Phi,\ \Upsilon,\ \Gamma],\right.\\ &\left.\left\{\left[x_{F,-1}^T,e^T\right]^T,u_{H,-1},\left[d^T,v^T\right]\right\}\right),\forall d\in\mathcal{D},v\in\mathcal{V},e\in\mathcal{H}\Big\}\subset\mathcal{E}_{i-1}\end{aligned}$$

where $x_{F,-1}\in\mathcal{E}_i$ and $u_{H,-1}$ are the stored estimate information and feasible command at the previous time instant, respectively. Therefore, the detection logics is:

$$\mathbf{D}_X^+(x_F(t)):=\begin{cases}\text{attack}, & \text{if } x_F(t)\notin\mathbf{Z}^+\left(x_{F,-1},u_{H,-1}\right)\\ \text{no attack, otherwise}\end{cases}$$

C. Smart Actuator

First, the actions of this unit can be summarized as follows: 1) identify the nature of the received signal $u(t)$; 2) store updated data; 3) apply an admissible input $u^{feas}(t)$ to the plant P. As the first point is concerned, this device is instructed to recognize the class of the received packed according to the following logic:

$$u^{feas}(t)=\begin{cases}u_H(t), & \text{If } dim(u(t))=1\\ \mathbf{u}_{(stored)_k}^{MPC}, & \text{If } dim(u(t))>1\\ u(t-1), & \text{If } \mathbf{D}_U^+(x_F(t),u(t))=\text{ attack}\end{cases}$$

In order to make easy the packet classification, the controller side sends the sequence $\bar{\mathbf{u}}(t)$ built as reported in Table I.

TABLE I

SEQUENCE DIMENSION *versus* DATA STRUCTURE

$dim(\bar{\mathbf{u}}(t))$	$\bar{\mathbf{u}}(t)$
1	$u_H(t)$
N	$\mathbf{u}_R^{MPC}(t)$
$N+1$	$\left\{\mathbf{u}_{M^1}^{MPC}(t),0_{n_u}\right\}$
$\vdots$	$\vdots$
$N+L$	$\left\{\mathbf{u}_{M^L}(t),\overbrace{0_{n_u},\ldots,0_{n_u}}^{L}\right\}$

The following reasoning applies. Once the packet $u(t)$ is received, the **Smart Actuator** checks its dimension: if $dim(\bar{\mathbf{u}}(t))$, then the **Actuator detector** is activated: if $u_H(t)$ is applied, then the stored command is updated, i.e., $u(t-1)\leftarrow u_H(t)$, otherwise the packet $\left\{y^s(t),0_{n_y}\right\}$ is transmitted to make aware the remote side that an attack is underway on the *controller-to-actuator* channel. Conversely if $dim,(u(t))=N$, an attack has been detected on the controller side and the sequence of resilient moves $\mathbf{u}_R^{MPC}(t)$ has been safely sent (in virtue of **Assumption 1**): it is stored $\mathbf{u}_{stored}^{MPC}\leftarrow\mathbf{u}_R^{MPC}(t)$ and completely driving the regulated state trajectory inside Ξ_0 where the state estimate feedback law $g_\Omega(0_x)=K_Hx_F(t)$ can be indefinitely applied. The same reasoning applies to the maintenance scenarios with Π_0^i in place of Ξ_0 and $g_i(x_i^e)=K_{M^i}(x_F(t)-x_i^e)+u_i^e$.

D. Smart Deconvolutor

The primary aim of this unit is to provide a state estimate $x_F(t)$ by exploiting the input and output data, $\bar{\mathbf{u}}(t)$ and $y(t)$, respectively. Unfortunately, communictaion links are unreliable and, therefore, whenever an attack is detected by the **Actuator Detector** this information must be available on the controller side for resilient/maintenance operations. Accordingly, the **Smart Deconvolutor** recognizes the attack occurrence on the plant side by simply analyzing the dimension of the received data $y(t)$, i.e. $dim(y(t))=2$.

Accordingly, the **Controller Detector** is skipped and one the following actions takes place:

$$\begin{cases} \text{If } x_{F,-1} \in \bigcup_{j=1}^{N} \Xi_j, \quad \text{then compute } \mathbf{u}_R^{MPC}(t) \\ \text{If } x_{F,-1} \in \bigcup_{j=1}^{N} \Pi_i^i, \quad \text{then compute } \mathbf{u}_{M^i}^{MPC}(t) \end{cases} \tag{22}$$

V. Numerical Example

Consider a differential drive-robot described by a noisy driven nonlinear continuous-time model fully reported in [18], where $p_x(t)$, $p_y(t)$ denote the lateral/longitudinal positions and $\theta(t)$ the cart attitude, while $\omega_r(t)$, $\omega_l(t)$ account for the right and left angular velocities (control signals). Moreover, the lateral and longitudinal positions satisfy the following constraints: $|\omega_r(t)| \leq 2[rad/sec], |\omega_l(t)| \leq 2[rad/sec]$. The measured output consists in the lateral and longitudinal positions; the process noise and the measurement errors are gaussian unitary variance white stochastic processes. The plant dynamics is embedded within a 4-vertices polytopic linear differential inclusion and discretized with a ZOH scheme by choosing the sampling time equal to $T_s = 0.1$ sec. The following operating scenario is hypothesized: 1) **Normal OP** : Zero lateral and longitudinal positions (the attitude is zero according to a *modulo* $2\,\pi$ rule); 2) **Maintenance OP** : Parking spot $[-1.7 \;\; -2.1]$ near a superellptic trajectory centered around the Normal OP. The control horizon length has been selected as $N = 40$. The numerical simulations have been performed over a $600 \;\; sec$ time horizon, the initial state estimate of the cart is $[1, \; 0.3, \; 0]$ (the real initial state is $[4, \; 4, 0]$ and three distinct diagnostic scenarios are performed (for the sake of space depicted on the same graph): **Healthy** - absence of attacks; **Maintenance** - attack along the actuator channel over the time window $[50, \;\; 150]$ sec .; **Resilient** - attack along the sensor measurement channel over the time window $[250, \;\; 350] \;\; sec$. By comparing the dynamical behaviors of the three operating scenarios and, as expected, the maintenance mode leads to the worst performance, see the red dotted line in Fig. 2. This is clearly due to the fact that the vehicle moves towards the "parking spot" $x^e = [-1.7 \;\; -2.1]^T$. Conversely, within the resilient mode, the vehicle keeps the zero target (orange dotted line) at a price of more conservative performance with respect to the completely healthy behavior (continuous blue line).

VI. Conclusions

In this paper, a control architecture based on the design of a state estimate model predictive control scheme has been presented for cyber-physical systems subject to malicious external actions on the communication links. One of the most relevant features of the proposed solution relies on its capability to keep the plant "alive" regardless of the occurrence of severe attacks and without resorting to communication refresh procedures.

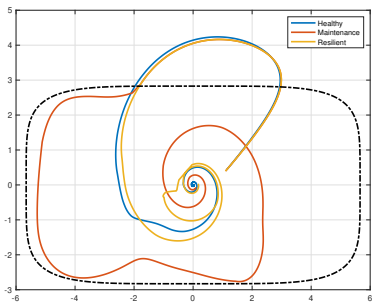

Fig. 2. Regulated state estimate trajectories projected on the positions plane (Healthy, Maintenance, Resilient)

References

[1] Y.Liu, Y. Peng, B. Wang, S. Yao and Z. Liu, "Review on cyber-physical systems", *IEEE/CAA J. Auto. Sin.*, Vol. 4, No. 1, pp.27-40, 2017.

[2] D. Ding, Q. L. Han, X. Ge, and J. Wang, "Secure state estimation and control of cyber-physical systems: A survey," *IEEE Trans. on Sys. Man, and Cyb.: Systems*, Vol 51, No. 1, pp. 176-190, 2021.

[3] T. Arauz, P. Chanfreut and J. M. Maestre, "Cyber-security in networked and distributed model predictive control", *Annual Reviews in Control*, Vol. 53, pp. 338-355, 2022.

[4] G. Franzè, W. Lucia, and F. Tedesco, "Resilient model predictive control for constrained cyber-physical systems subject to severe attacks on the communication channels," *IEEE Transactions on Automatic Control*, Vol. 67, No. 4, pp. 1822-1836, 2022.

[5] R. Romagnoli, B. H. Krogh, D. de Niz,A. D. Hristozov and B. Sinopoli, "Software Rejuvenation for Safe Operation of Cyber–Physical Systems in the Presence of Run-Time Cyberattacks," *IEEE Trans. on Contr. Sys. Tech.*, Vol. 31, No.4, pp.1565-1580, 2023.

[6] Y.-C. Sun and G.-H. Yang, "Robust event-triggered model predictive control for cyber-physical systems under denial-of-service attacks," *Int. J. Rob. and Nonl. Contr.*, Vol. 29, No.14, pp. 4797-4811, 2019.

[7] G. Franzè, F. Tedesco and W.Lucia, "Resilient control for cyber-physical systems subject to replay attacks," *IEEE Control Systems Letters*, Vol. 3, No. 4, pp.984-989, 2019.

[8] S. Chen, Z. Wu and P. D. Christofides,"Cyber-attack detection and resilient operation of nonlinear processes under economic model predictive control", *Comp. & Ch. Eng.*, Vol. 136, 106806, 2020.

[9] J. Wang, B. Ding and J. Hu,"Security control for LPV system with deception attacks via model predictive control: A dynamic output feedback approach", *IEEE Transactions on Automatic Control*, Vol. 66, No. 2, pp. 760-767, 2020.

[10] G. Franzè, D. Famularo, W. Lucia and F. Tedesco,"Cyber–physical systems subject to false data injections: A model predictive control framework for resilience operations," *Autom.*, Vol. 152, 110957, 2023.

[11] A. Casavola, D. Famularo and G. Franzè, "A robust deconvolution scheme for fault detection and isolation of uncertain linear systems: an LMI approach", *Automatica*, Vol. 41, No. 8, pp. 1463-1472, 2005.

[12] D. Angeli, A. Casavola, G. Franzè and E. Mosca, "An Ellipsoidal Off-line MPC Scheme for Uncertain Polytopic Discrete-time Systems", *Automatica*, Vol. 44, pp. 3113–3119, 2008.

[13] F. Blanchini and S. Miani,"Set-Theoretic Methods in Control", *Birkäuser*, Boston, 2008.

[14] H. D. Tuan, P. Apkarian, and T. Nguyen, "Robust filtering for uncertain nonlinearly parameterized plants," *IEEE Transactions on Signal Processing*, vol. 51, no. 7, pp. 1806–1815, 2003.

[15] E. Fridman and U. Shaked. "Delay-dependent H-infinity control of uncertain discrete delay systems", *EJC* , Vol. 11, pp. 29–37, 2005.

[16] G. Franzè, F. Tedesco, and D. Famularo, "Model predictive control for constrained networked systems subject to data losses", *Automatica*, vol. 54, pp. 272–278, 2015.

[17] V. Varadharajan, U. Tupakula and K. K. Karmakar, "Techniques for Enhancing Security in Industrial Control Systems", *ACM Transactions on Cyber-Physical Systems*, Vol. 8, No. 1, pp. 1-36, 2024.

[18] C. Tiriolo, G. Franzé and W. Lucia,"An Obstacle-Avoidance Receding Horizon Control Scheme for Constrained Differential-Drive Robot via Dynamic Feedback Linearization", ACC 2023, San Diego, USA, pp. 1116-1121, 2023.