Available online at www.sciencedirect.com

ScienceDirect

IFAC PapersOnline CONFERENCE PAPER ARCHIVE

IFAC PapersOnLine 55-6 (2022) 278–284

Resilient tube-based MPC for Cyber-Physical Systems Under DoS Attacks [1]

B. Aubouin–Pairault * **A. Perodou** * **C. Combastel** *
A. Zolghadri *

* *Univ. Bordeaux, CNRS, IMS, UMR 5218, 33405 Talence, France*

Abstract: This paper proposes a resilient and robust model predictive control (MPC) scheme for a class of Cyber-Physical Systems (CPS) subject to state and input constraints, unknown but bounded disturbances and Denial of Service (DoS) attacks. The attacker blocks the controller to actuator communication and the attacks are assumed to be time-limited. The control is designed by extending a robust tube-based MPC, where a new type of invariant set, namely μ-step Robust Positively Invariant (μ-RPI) set, is introduced to deal with resilience. A set-based method is then developed for the control scheme to ensure both resilience to DoS attacks while preserving robustness to bounded disturbances. A computational algorithm is derived and a numerical example is provided to illustrate the potential of the proposed approach.

Keywords: Cyber-Physical Systems (CPS), Denial of Service (DoS) attack, Resilience, Robustness, Model Predictive Control (MPC), Set-membership, Zonotopes.

1. INTRODUCTION

Cyber-Physical Systems (CPSs) are next-generation engineered systems with deep integration of computation, communication and networking, physical processes, and control systems (Lee (2015), Poovendran et al. (2011), Allgöwer et al. (2019)). Varying widely in complexity and scale, CPSs concern many technological areas, including aerospace, automotive, energy, chemical industry, transportation, or healthcare. While safety and security have been traditionally addressed separately, some integrated approaches have been recently reported (see for instance Ji et al. (2021) and the references therein).

In this perspective, this paper focuses on mitigating the impact of denial of services (DoS) attacks on systems evolving in an uncertain environment. In the literature, one can find many investigations for mitigation of DoS attacks. Among others, in Gupta et al. (2016) a method is proposed based on game theory where both attacker and controller are modeled as players of a game. De Persis and Tesi (2015) used event-triggered control, and the approach reported in Amin et al. (2009) takes advantage of optimal control. Nevertheless few of them deal with systems subject to state and input constraints. Sun et al. (2019) proposed a resilient MPC to address DoS attacks for a constrained system but without taking disturbances into account. In this paper, a similar resilient MPC is extended to disturbed systems with the aim of ensuring a joint resilience and robustness goal. By resilience, it is meant the system's ability to contain the maximal impact of anomalies, such as attacks, and to recover to an acceptable performance level.

In order to characterize the impact of uncertainties, a set-membership approach is used. This deterministic approach has been used in various ways when dealing with systems subject to unknown but bounded uncertainties. For instance, state bounding observation through Zonotopic Kalman Filters (ZKF) is considered in Combastel (2015). In Mayne et al. (2006) a robust model predictive controller is proposed, and in Le et al. (2011) a zonotopic tube-based approach is used to control a system subject to disturbances and measurement noise. In the last two papers, a particular class of invariant sets, the Robust Positively Invariant (RPI) set, is defined to ensure the robust convergence of the control scheme in the presence of bounded uncertainties. Franze et al. (2021) also studied set membership theory and MPC to control constrained and disturbed linear systems subject to different possible attacks. The resilient approach we propose mainly relies on zonotopic rather than ellipsoidal sets. It ensures that the state trajectory comes back within some set after a DoS attack sequence, as in Franze et al. (2021). Moreover, an explicit bound for the state trajectory during attacks is also considered.

In this paper, a new kind of sets, namely μ-step Robust Positively Invariant (μ-RPI) sets, is introduced to address the resilience issue, that is, ensuring that an exit from nominal operation induced by the possibly repeated occurrence of attacks remains limited in time and/or magnitude. Then, a resilient tube-based model predictive control for uncertain linear discrete-time systems subject to DoS attack and bounded disturbances is proposed. The resulting MPC scheme relies on the off-line computation of such an

[1] This work has been done when all the authors were with the University of Bordeaux, IMS-lab, CNRS UMR 5218, Bat. A31, 351 cours de la Libération, 33400, Talence, France. Emails: bob.aubouin-pairault@gipsa-lab.fr (corresponding author), arthur.perodou@ec-lyon.fr, {christophe.combastel, ali.zolghadri}@ims-bordeaux.fr .

10.1016/j.ifacol.2022.07.142

μ-RPI set for which an algorithmic solution is provided, taking into account all design constraints.

The paper is organized as follows. After some preliminaries given in Section 2, the problem is stated in Section 3. Section 4 describes the proposed control scheme and Section 5 presents a method to compute the required μ-RPI set. Finally an illustrative example is provided in Section 6, and Section 7 provides some concluding remarks.

2. PRELIMINARIES

Notations: The symbols $\mathbb{R}, \mathbb{N}$ and $\mathbb{N}^+$ represent respectively the sets of real numbers, natural numbers, and positive integers. $[\![k_1, k_2]\!]$ denotes the set of integers between, and including, k_1 and k_2. The operators $\oplus$ and $\ominus$ denote the Minkowski sum and difference. Given the sequence of sets $\{\mathbb{S}_i, \subset \mathbb{R}^n\}_{i=a}^b$, the notation $\bigoplus_{i=a}^b \mathbb{S}_i = \mathbb{S}_a \oplus ... \oplus \mathbb{S}_b$ is used. $P \succ 0$ (resp. $P \succeq 0$) denote a positive definite (resp. semi-definite) matrix. $\rho(A)$ denotes the spectral radius of the matrix A i.e. the largest eigenvalue in absolute value. Given a vector $x \in \mathbb{R}^n$ and $P \succ 0$, $x^\top$ denotes the transpose of the vector and the P-weighted norm is $||x||_P = \sqrt{x^\top P x}$. The notations $x_{k_1|k_2}$ and $u_{k_1|k_2}$ are used to describe state and control input predicted for time k_1 and calculated at time k_2.

A zonotope $\langle c, R\rangle \subset \mathbb{R}^n$ with center $c \in \mathbb{R}^n$ and generator matrix $R \in \mathbb{R}^{n\times p}$ is a polytopic set defined as the affine image of the unit hypercube $[-1, +1]^p \subset \mathbb{R}^p$ by R: $\langle c, R\rangle = \{c + Rs, ||s||_\infty \leq 1\}$. The Minkowski sum of two zonotopes $\langle c_1, R_1\rangle$ and $\langle c_2, R_2\rangle$ is the zonotope $\langle c_1, R_1\rangle \oplus \langle c_2, R_2\rangle = \langle c_1 + c_2, [R_1, R_2]\rangle$. The linear image of $\langle c, R\rangle$ by L is the zonotope $L \odot \langle c, R\rangle = \langle Lc, LR\rangle$. The interval/box hull of $\langle c, R\rangle$ is the interval $c \pm |R|\mathbf{1}$ where $c \pm r$ denotes the interval $[c - r, c + r]$, $|.|$ is the element-by-element absolute value operator, and $\mathbf{1}$ is a column of ones with appropriate size, Combastel (2003).

3. PROBLEM STATEMENT

3.1 System Dynamics

A linear dynamic subject to bounded disturbances is first considered:

$$x_{k+1} = Ax_k + Bu_k + Dw_k, \tag{1}$$

where $x_k \in \mathbb{R}^n$, $u_k \in \mathbb{R}^m$, and $w_k \in \mathbb{R}^l$ are respectively the system state, the control input and the disturbances evaluated at time k. It is assumed that the disturbances are bounded: $w_k \in \mathbb{W}$ and the system state and control input satisfy constraints $x_k \in \mathbb{X}$ and $u_k \in \mathbb{U}$, where $\mathbb{X}$ and $\mathbb{U}$ are compact sets containing the origin as an interior point.

Assumption 1. There exists a state-feedback gain K such that $A + BK$ is stable, that is $\rho(A + BK) < 1$.

3.2 Attack Model

The equation (1) is modelling the attack-free dynamic of a CPS where actuator and controller are spatially separated (e.g. remote control) while being connected through communication channel. In this paper, the case of a DoS attack occurring on this channel is considered. More precisely, the scenario considered here is time limited attacks which block the controller-actuator (C-A) communication channel. The indicator variable $\nu_k, k \in \mathbb{N}$, is defined as follows:

$$\nu_k = \begin{cases} 1 \text{ while there is no attack,} \\ 0 \text{ when an attack occurs.} \end{cases} \tag{2}$$

Then, the applied input is $u_k = \nu_k u_k^c$ where u_k^c is the control input computed by the controller.

Assumption 2. $\forall k_j \in \mathbb{N}$, the constraint on the occurrence of attacks is the following:

$$\sum_{k=k_j}^{k_j+N-1} (1 - \nu_k) \leq M < N, \tag{3}$$

where M denotes the maximal number of sample attack instances on the time interval from k_j to $k_j + N - 1$.

This assumption could model power-limited attacks where the attacker can launch a maximal occurrence of attacks over a time period. M consecutive attacks are not necessarily the worst-case scenario, the assumption considers all the possible scenarios with at most M attacks over N sample times. Indeed, under assumption 2, distinct consecutive DoS attack sequences are possible within the considered time horizon, as illustrated in Fig. 3. In this paper, the number N matches with the time-horizon of the MPC scheme that will be introduced in next section.

3.3 Resilient sets and problem statement

In order to deal with the resilience property for a system subject to disturbances and attacks, a new kind of invariant set is proposed in this subsection. First, the definition of a Robust Positively Invariant (RPI) set is recalled:

Definition 1. (RPI set, Rakovic et al. (2005)). Given a dynamic system $x_{k+1} = f(x_k, w_k)$, the set $\mathbb{S}$ is said to be Robust Positively Invariant (RPI), if $f(x, w) \in \mathbb{S}$ for all $x \in \mathbb{S}$ and all $w \in \mathbb{W}$.

A resilient and robust invariant set, that both generalizes the usual RPI set and the μ-step invariant set originally proposed in Sun et al. (2019), is now introduced:

Definition 2. (μ-RPI set). Given a system Σ modelled as $x_{k+1} = f(x_k, w_k)$, if $\exists \mu \in \mathbb{N}^+$ such that the implication (4) is satisfied, then the set $\mathbb{S}$ is said to be μ-step Robust Positively Invariant (μ-RPI set) for Σ,

$$((x_0 \in \mathbb{S}) \wedge (\forall k \in \mathbb{N},\, w_k \in \mathbb{W})) \Rightarrow \forall k \in \mathbb{N},\, x_{\mu+k} \in \mathbb{S}. \tag{4}$$

Given the system (1) subject to a DoS attack modeled by (2), the problem addressed is that of finding a resilient and robust model predictive control scheme for which an μ-RPI set exists, and compute this set. By this way, the purpose is to obtain a provenly stable control scheme which is *jointly* resilient to attacks as described in the paragraph 3.2 *and* robust to any arbitrary bounded disturbances $w_k \in \mathbb{W}$.

4. A ROBUST AND RESILIENT MPC SCHEME

In this section, a standard robust tube-based MPC is first briefly recalled. Then, a recent proposition of MPC scheme providing resilience to a non-disturbed LTI system under

DoS attacks is reviewed. Finally, an original MPC scheme combining both robustness *and* resilience is proposed.

4.1 Tube-based MPC

In standard robust tube-based MPC, the objective is to control the system (1) such that its states remain in a tube centered on a nominal trajectory. Consider the following nominal model:

$$\bar{x}_{k+1} = A\bar{x}_k + B\bar{u}_k. \tag{5}$$

Then, the general idea is to ensure that the disturbed system state x_k stays close to $\bar{x}_k$, for any arbitrary disturbances belonging to $\mathbb{W}$. To achieve this goal, the nominal system is controlled using MPC with tightened constraints and the control law (6) is applied to the disturbed system:

$$u_k = \bar{u}_k + K(x_k - \bar{x}_k). \tag{6}$$

If K is chosen such that $(A+BK)$ is stable, the difference $x_k - \bar{x_k}$ can be bounded in a Robust Positively Invariant (RPI) set and thus creates a tube around the nominal state trajectory that encloses the disturbed state trajectories as described in Rawlings and Mayne (2009). Note that this is a simple version of the tube-based MPC where the nominal system is completely independent of the state trajectory and that improved versions of this control method exist (see Rawlings and Mayne (2009)).

4.2 Resilient MPC

This paragraph is intended to provide a short synopsis of the resilient MPC for non-disturbed systems as proposed in Sun et al. (2019). In a classical MPC scheme, at each step time, the optimal sequence of control inputs $\mathbf{u}_k^*$ is computed over the whole N samples prediction horizon and only the first term $u^*_{k|k}$ is applied to the system. In order to mitigate the impact of DoS attacks, Sun et al. (2019) made the assumption that the actuator side is able to store data and the computed control sequence $\{u^*_{k|k}, u^*_{k+1|k}, .., u^*_{k+N-1|k}\}$ is sent to the actuator at each sample time. Thus, when a DoS attack impedes the reception of the optimal control at some time k, the actuator can still apply the next control stored in the previously received control sequence. Denoting k_j the last sample time before an attack occurs, the control applied to the disturbed system is $u^*_{k|k_j}$ which leads to the dynamic:

$$x_{k+1} = Ax_k + Bu^*_{k|k_j}. \tag{7}$$

In Sun et al. (2019), the stability of (7) is proved under assumption 2 and for a region of attraction $\mathbb{X}_N^M$. The later differs from that of a classical MPC by taking into account the case of an attack happening at a time when no control sequence is stored in the actuator side (just after the initialization of the controller, for instance). This set is such that for all $x_0 \in \mathbb{X}_N^M$, there exists a control sequence $\mathbf{u}^M = \{\underbrace{0, .., 0}_{M}, \underbrace{u_M, .., u_{N-1}}_{N-M}\}$ satisfying $x_N \in \mathbb{X}_f$ under the constraints $u_i \in \mathbb{U},\ \forall i \in [\![M, N-1]\!]$ and $x_i \in \mathbb{X},\ \forall i \in [\![1, N-1]\!]$, where $\mathbb{X}_f$ denotes the terminal set of the MPC problem.

4.3 Toward a robust and resilient control law

To provide both resilience and robustness, a new control law combining the previous tube-based MPC (§4.1) and resilient MPC (§4.2) is proposed. First, the constrained optimization problem which is solved to control the nominal system (5) is introduced:

MPC optimization: The cost function is given by:

$$V_N(\bar{x}_k, \bar{\mathbf{u}}_k) = ||\bar{x}_{k+N|k}||_S^2 + \sum_{i=0}^{N-1} ||\bar{x}_{k+i|k}||_Q^2 + ||\bar{u}_{k+i|k}||_R^2$$

where $\bar{\mathbf{u}}_k = \{\bar{u}_{k|k}, \bar{u}_{k+1|k}, .., \bar{u}_{k+N-1|k}\}$. and $Q, R, S \succ 0$. The constraints applied to the state and the control input of the nominal system are $\bar{\mathbb{X}} = \mathbb{X} \ominus \mathbb{Z}^+$ and $\bar{\mathbb{U}} = \mathbb{U} \ominus K\mathbb{Z}^+$, where $\mathbb{Z}^+$ denotes a set bounding the difference $z_k = x_k - \bar{x}_k$. Those tightened constraints applied to the nominal system ensure that the disturbed system (1) meets the specification $x_k \in \mathbb{X}$ and $u_k \in \mathbb{U}$.

In order to ensure the stability and feasibility of the considered MPC problem, a terminal set $\bar{\mathbb{X}}_f$ is also introduced (see Rawlings and Mayne (2009) for details). The terminal cost $||..||_S$ and the terminal set $\bar{\mathbb{X}}_f$ are chosen consistently according to assumption 3:

Assumption 3. There exists a state-feedback gain K such that, for the system $\bar{x}_{k+1} = (A+BK)\bar{x}_k$:

- There exists a terminal set $\bar{\mathbb{X}}_f \subset \bar{\mathbb{X}}$ also satisfying $(A+BK)\bar{\mathbb{X}}_f \subset \bar{\mathbb{X}}_f$ and $K\bar{\mathbb{X}}_f \subset \bar{\mathbb{U}}$,
- $||(A+BK)\bar{x}_k||_S^2 + ||\bar{x}_k||_Q^2 + ||K\bar{x}_k||_R^2 \leq ||\bar{x}_k||_S^2$.

Then, the MPC constrained optimization is given by:

$$\begin{aligned} \bar{\mathbf{u}}_k^* = \min_{\bar{\mathbf{u}}_k} \quad & V_N(\bar{x}_k, \bar{\mathbf{u}}_k) \\ \text{s.t.} \quad & \bar{x}_{k|k} = \bar{x}_k, \\ & \bar{x}_{k+i+1|k} = A\bar{x}_{k+i|k} + B\bar{u}_{k+i|k}, \\ & \bar{u}_{k+i|k} \in \bar{\mathbb{U}} \text{ for } i \in [\![0 : N-1]\!], \\ & \bar{x}_{k+i|k} \in \bar{\mathbb{X}} \text{ for } i \in [\![1 : N-1]\!], \\ & \bar{x}_{k+N|k} \in \bar{\mathbb{X}}_f. \end{aligned} \tag{8}$$

Resilience: Since attacks can occur, the robust control (6) may not be received by the actuators at some time steps. Similarly to Sun et al. (2019) and Franze et al. (2021), it is assumed that the actuator side is able to store data. Then, since only past measured states are available at each sample time k, the sequence $\{\bar{u}^*_{k|k} + K(x_k - \bar{x}_k), \bar{u}^*_{k+1|k}, .., \bar{u}^*_{k+N-1|k}\}$ is sent to the actuator at each sample time k. Denoting k_j the last sample time before an attack occurs and using ν_k as defined in (2), the control applied to the disturbed system is:

$$u_k = \bar{u}^*_{k|k_j} + \nu_k K(x_k - \bar{x}_k)$$

For the sake of simplicity, x_k is assumed available. Otherwise, an observer should be used. Then, the robustness to the related observation error should be properly handled. Moreover, in a similar fashion to (Amin et al. (2009)), the communication protocol is assumed to be acknowledgment-based like e.g. the TCP protocol (Kumar and Rai (2012)). Then, the controller has access to k_j and the nominal system can be controlled using $\bar{u}_k = \bar{u}^*_{k|k_j}$. With this control, the nominal system follows the dynamic

(7) already studied by Sun et al. (2019). The controlled nominal system is thus stable for a region of attraction $\bar{\mathbb{X}}_N^M$. This region of attraction $\bar{\mathbb{X}}_N^M$ is the same as in subsection 4.2, except that that the constraints on the states and the control inputs are given by the tightened constraints $\bar{\mathbb{X}}_f, \bar{\mathbb{U}}$ and $\bar{\mathbb{X}}$.

Robustness and Resilience: The proposed approach relies on a dedicated management of the state error between the disturbed (1) and nominal (5) system models, $z_k = x_k - \bar{x}_k$, which follows the dynamics:

$$z_{k+1} = (A + \nu_k BK)z_k + Dw_k \tag{9}$$

This is the subject of the main results developed in the next section.

5. MAIN RESULTS

In this section, an algorithmic solution is provided to test if a given RPI set for the dynamic (10),

$$z_{k+1} = (A + BK)z_k + Dw_k, \tag{10}$$

is also an $N-$RPI set for the dynamic (9) under attack scenarios characterized by the pair (M, N). As a byproduct, it will thus be possible to determine the maximal value of $M < N$ ensuring a resilient MPC control. Moreover, a solution for computing a set $\mathbb{Z}^+$ bounding the trajectories of the state error z_k is proposed. $\mathbb{Z}^+$ is represented as an intersection of halfspaces and characterizes the worst-case impact of the specified disturbances and attacks with respect to the nominal state trajectory.

5.1 Testing if an RPI set is also an N-RPI set

In this section, $\mathbb{P}$ denotes an RPI set for the system (10). It can be computed as an approximation of the minimal RPI set of (10), as proposed in Rakovic et al. (2005).

The aim of this paragraph 5.1 is to test if $\mathbb{P}$ is also an N-RPI set for system (9). Indeed, since the condition (3) applies to sequences of N steps, a solution to ensure the resilience to repeating sequences of any length consists in focusing on μ-RPI sets with $\mu \leq N$ (thus, on N-RPI sets), as illustrated in Fig. 1.

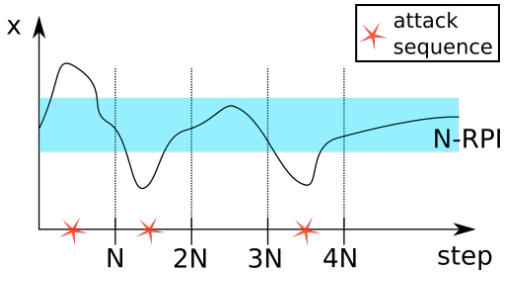

Fig. 1. Illustration of the usage of the N-RPI

To achieve this, the proposed method consists in testing if, for each considered attack scenario, the trajectory gets back into $\mathbb{P}$ in a maximum of N steps. Instead of testing all the possible attack scenarios, a sufficient subset is introduced in the sequel. In addition to reduce the algorithmic complexity, there is no loss of generality to prove, or disprove, that $\mathbb{P}$ is an N-RPI set when testing only this subset. This relevant subset is obtained as follows:

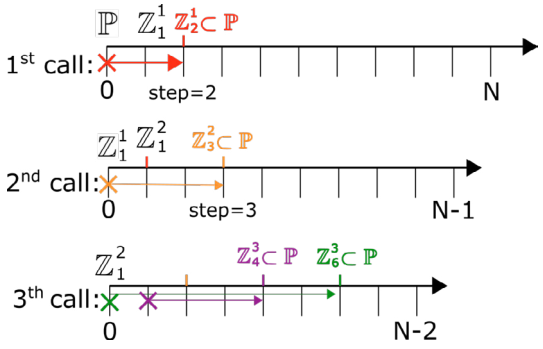

Fig. 2. Illustration of Algorithm 1

- Only the scenarios where the first attack happens at the first of N consecutive samples is tested. This is a direct consequence of Assumption 2, where the considered class of attacks satisfies (3) for time-horizon N.
- If, for i sample attack instances with the last attack happening at step k_a, the system gets back to the RPI set in a total of k_b steps, then, to test a scenario with $i+1$ attack instances where the first i attacks are the same, testing only the scenarios where the last attack happens between $k_a + 1$ and $k_b - 1$ is sufficient.

Using the above rules, a sufficient subset of scenarios to be tested can be constructed. First, starting from an RPI set $\mathbb{P}$ at $k = 0$ and with one sample attack happening at this time, a minimal number k_b of steps (up to N) required for the system trajectories to provenly get back to $\mathbb{P}$ is determined. Then, the expression of the reachable set is computed as follows:

$$\begin{cases} \mathbb{Z}_0^1 = \mathbb{P}, & \\ \mathbb{Z}_{k+1}^1 = A\mathbb{Z}_k^1 \oplus D\mathbb{W}, & \text{if } \nu_k = 0, \\ \mathbb{Z}_{k+1}^1 = (A+BK)\mathbb{Z}_k^1 \oplus D\mathbb{W}, & \text{otherwise.} \end{cases} \tag{11}$$

Where $\mathbb{Z}_k^j$ is the set reached during the k^{th} step for a scenario j. To test the scenarios with two sample attack instances, the initial set is given by $\mathbb{Z}_0^2 = \mathbb{Z}_1^1$ and the scenarios considered are the ones where an attack occurs at time k with $k \in [\![0, k_b - 2]\!]$. The number of sample attacks is then incremented until it reaches M which is necessary for the test to succeed unless a set-inclusion test fails.

Algorithm 1 is a recursive function that tests if an RPI set $\mathbb{P}$ is also an N-RPI set for attack scenarios described by the integers (M, N). Each call of the recursive function tests all the required scenarios, starting from the set $\mathbb{Z}_0$ with an attack happening between step 0 and step $n_{step} - 1$, where n_{step} is a number of steps passed as input argument (with initial value one) when calling the isNRPI function. For a scenario with an attack happening at time k_a, and the trajectories entering in the RPI set in less than N steps, in k_b steps for instance. The recursive function is recalled to test new scenarios starting from the set $\mathbb{S} = \mathbb{Z}_{k_a+1}$ and it tests that the trajectories will come back in the RPI set in less than $N - k_a - 1$ steps with an attack happening between the steps 0 and $k_b - 2 - k_a$. The function stops if a trajectory does not enter in the RPI before the maximum allowed step number or if there is no more attack to test i.e. the last scenarios tested already include the cases with M sample attacks.

For the sake of illustration, the operation of Algorithm 1 is exemplified in Fig. 2 where:

- During the first call, a scenario starting from $\mathbb{P}$ with an attack at the first step is considered. The trajectories get back to $\mathbb{P}$ in 2 steps.
- The function is recalled and a scenario starting from $\mathbb{Z}_1^1$ with an attack at the first step is considered. The trajectories get back to $\mathbb{P}$ in 3 steps.
- During the third call of the function, two scenarios are studied. Both start from the set $\mathbb{Z}_1^2$ and one contains an attack at the first step and the other one an attack at the second step. The two trajectories from the scenarios come back in $\mathbb{P}$ in less than $N-2$ steps which is the limit for those trajectories.

Algorithm 1 Test if a RPI $\mathbb{P}$ is a N-RPI for a given number M of sample attacks over the horizon N

function $[test, b]$ = isNRPI(M, N, $\mathbb{P}$, $\mathbb{Z}_0$, n_{step}, b)
if ($\mathbb{Z}_0$, n_{step}, b) is undefined **then** ▷ Initialization
  $\mathbb{Z}_0 \leftarrow \mathbb{P}$ ▷ where $\mathbb{P}$ has to be a RPI set
  $n_{step} \leftarrow 1$ ▷ First attack happens at time k=0
  $b = (-\infty)\mathbf{1}$ ▷ col. vector with $-\infty$ elements
end if
if $(M = 0)$ **then** ▷ Stop criterion for recursive calls
  $test \leftarrow True$
else
  $k_a \leftarrow 0$ ▷ Sample attack time-step
  $Cond_1 \leftarrow True$
  while $Cond_1$ **do**
    $i \leftarrow 0$ ▷ Time-step index
    $\mathbb{Z} \leftarrow \mathbb{Z}_0$
    $Cond_2 \leftarrow True$
    while $Cond_2$ **do**
      if $(i = k_a)$ **then** ▷ Set reached under attack
        $\mathbb{Z} \leftarrow A\mathbb{Z} \oplus D\mathbb{W}$
        $\mathbb{S} \leftarrow \mathbb{Z}$ ▷ Save set after attack
      else ▷ Set reached without attack
        $\mathbb{Z} \leftarrow (A + BK)\mathbb{Z} \oplus D\mathbb{W}$
      end if
      $b \leftarrow UpdateBound(H, b, \mathbb{Z})$ ▷ Update $\bar{\mathbb{Z}}^+$
      $i \leftarrow i + 1$
      $Cond_2 \leftarrow (i < N) \wedge \neg(\mathbb{Z} \subset \mathbb{P})$
    end while
    $k_b \leftarrow i$
    if $(\mathbb{Z} \subset \mathbb{P})$ **then**
      ▷ When back to $\mathbb{P}$ in less than N steps, then
      ▷ recursive call with one less sample attack
      ▷ and k_a less steps to get back to $\mathbb{P}$ starting
      ▷ from $\mathbb{S}$:
      $(test, b) \leftarrow$ isNRPI($M-1$, $N-k_a-1$, $\mathbb{P}$, $\mathbb{S}$, k_b-1-k_a, b)
    else
      $test \leftarrow False$
    end if
    $k_a \leftarrow k_a + 1$
    $Cond_1 \leftarrow (k_a < n_{step}) \wedge (test)$
  end while
end if
return $test, b$

The implementation of Algorithm 1 makes use of zonotopes to represent the RPI set and the sets reachable by the trajectories. This representation is well-suited in this case since it is closed for the Minkowski sum and affine image operators which can be easily computed (see §2). To test the containment of zonotopes at step 25 of Algorithm 1, the algorithm presented in Kulmburg and Althoff (2021) and implemented in the CORA 2021 toolbox is used. Note also that the step 23 in Algorithm 1 is used to compute a set bounding all the trajectories as further described in the next paragraph 5.2.

5.2 Bound of trajectories

The aim of this paragraph is to compute an outer approximation $\bar{\mathbb{Z}}^+$ of the set $\mathbb{Z}^+$ bounding the trajectory error with respect to the nominal model, under both bounded disturbances and the specified attacks. Following (9) with $z_0 \in \mathbb{P}$, where $\mathbb{P}$ is N-RPI as tested by Algorithm 1, $\mathbb{Z}^+$ is given by (12):

$$\mathbb{Z}^+ = \bigcup_{i=1}^{n_Z} \mathbb{Z}_i, \tag{12}$$

where $\mathbb{Z}_i,\ i \in [\![1, n_Z]\!]$ denotes the collection of the sets $\mathbb{Z}$ computed at steps 18 and 21 during all the iterations within Algorithm 1 i.e. during the recursive exploration of the required scenarios. Since zonotopes are not closed for union, $\mathbb{Z}^+$ is not a zonotope. To compute an outer approximation $\bar{\mathbb{Z}}^+$ of $\mathbb{Z}^+$, a polytope in H-representation (i.e. intersection of half-spaces) can be used, $\bar{\mathbb{Z}}^+ = \{z \mid Hz \leq b\}$, and efficiently updated (see step 23 in Algorithm 1, and Algorithm 2). The half-space directions are predefined in a constant matrix $H \in \mathbb{R}^{d \times n}$ whose rows are made of d unitary vectors uniformly distributed on an n-dimensional unit hypersphere e.g. as in Marsaglia (1972). If needed, H can be appended with other specific directions such as those related to the canonical basis, for instance.

Then, $\bar{\mathbb{Z}}^+ \supset \mathbb{Z}^+$ is obtained by the iterative update called at step 23 in Algorithm 1. The iteration itself is described in Algorithm 2. For each computed zonotope $\mathbb{Z}$ (like $\mathbb{Z}_i$ in (12)), it consists in computing a tight inflation of the bounding vector b so that $\mathbb{Z} \subset \bar{\mathbb{Z}}^+$ is satisfied. This is basically achieved using the support point and interval hull properties of zonotopes, as expressed in vector form in the body of Algorithm 2.

Algorithm 2 Tight update of half-space bounds of polytope $\bar{\mathbb{Z}}^+ = \{z \mid Hz \leq b\}$ to include the zonotope $\mathbb{Z} = \langle c, R \rangle$

function b = UpdateBound($H, b, \langle c, R \rangle$)
$b \leftarrow max(b, Hc + |HR|\mathbf{1})$ ▷ $\mathbf{1}$ is a col. vec. of ones
return b

Finally, once the test implemented in Algorithm 1 successfully terminates, the iterative calls of Algorithm 2 result in an intersection of halfspaces, i.e. a polytope, bounding all the trajectories starting from the N-RPI set $\mathbb{P}$. Note that, by definition 2, all these trajectories also get back to $\mathbb{P}$ in at most N steps, no matter how the specified attacks and the bounded disturbances change in time.

5.3 Robust and Resilient MPC

For the implementation of the robust and resilient control scheme introduced in Section 4, the objective is to find a sufficiently small N-RPI to ensure that the difference between the system dynamic (1) and the nominal model

(5) meets an acceptable control accuracy (i.e. the required level of precision during normal operation). Moreover, the smaller the N-RPI is, the smaller the trajectory bounding set $\mathbb{Z}^+$ will be, so leading to less restrictive tightened constraints $\bar{\mathbb{X}} = \mathbb{X} \ominus \mathbb{Z}^+$ and $\bar{\mathbb{U}} = \mathbb{U} \ominus K\mathbb{Z}^+$ for the MPC control of the nominal model. Also, the larger the N-RPI set is, the larger will be the allowable disturbance bounds and/or the maximum number M of sample attacks as in (3). Thus, for a given scenario, the parameterized (by α) family of sets $\mathcal{F}_{\mathbb{P}} = \{\alpha\mathbb{P} \mid \alpha \geq 1\}$ is considered and the objective is then to find the smallest α such that the set $\alpha\mathbb{P}$ is N-RPI for the considered system and scenarios. $\mathcal{F}_{\mathbb{P}}$ is considered because any linear inflation of an RPI set by a scalar factor greater than one is also an RPI set. As a result, the proposed Resilient and Robust MPC can be set as follows:

a) Compute a stable K (e.g. as an LQ solution),
b) Compute $\mathbb{P}$ as described in Rakovic et al. (2005),
c) Find α s.t. $\alpha\mathbb{P}$ is N-RPI (§5.1) and compute $\bar{\mathbb{Z}}^+$ (§5.2),
d) Compute $\bar{\mathbb{X}}$ and $\bar{\mathbb{U}}$ (polytopic tightened constraints),
e) Compute S as a solution of the Lyapunov equation:
$$(A+BK)^\top S(A+BK) - S = -(Q+K^\top RK), \quad (13)$$
f) Compute β s.t. the terminal set $\bar{\mathbb{X}}_f = \{x \in \mathbb{R}^2 \mid ||x||_S^2 < \beta\}$ satisfies $\bar{\mathbb{X}}_f \subset \bar{\mathbb{X}}$ and $K\bar{\mathbb{X}}_f \subset \bar{\mathbb{U}}$.

Note that Algorithm 1 can be called within a dichotomy search to minimize α at step c). Also, e) and f) are focused on the approach concretely used in section 6 to obtain a final weight and terminal set satisfying the requirements of Assumption 3, where the invariance of $\bar{\mathbb{X}}_f$ as in f) is ensured by (13).

6. NUMERICAL EXAMPLE

Consider a second order system modelling the attack-free dynamic of a CPS as given by (1) and as explained in section 3 with:

$$A = \begin{bmatrix} 1.05 & 0.5 \\ -0.6 & 1.1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad D = \begin{bmatrix} 1 \\ 0.5 \end{bmatrix}$$

With the state constraint $\mathbb{X} = \{x \in \mathbb{R}^2 \mid ||x||_\infty \leq 20\}$, the control input constraint $\mathbb{U} = \{u \in \mathbb{R} \mid ||u||_\infty \leq 7\}$, and the disturbance set $\mathbb{W} = \{w \in \mathbb{R} \mid ||w||_\infty \leq 0.1\}$. For the MPC problem, Q is the identity matrix, $R = 0.1$, and the prediction horizon is set to $N = 10$. Then, K is calculated as a solution of the LQ problem with the previous costs. This results in $K = \begin{bmatrix} -0.6359 \\ -0.6740 \end{bmatrix}^\top$.

With those parameters, an ε-approximation of the minimal RPI set $\mathbb{P}$ is first obtained using the formula :

$$\mathbb{P}(s,\gamma) = (1-\gamma)^{-1} \bigoplus_{i=0}^{s-1} (A+BK)^i D\mathbb{W},$$

as proposed in Rakovic et al. (2005), with $\gamma = 0.01$ and $s = 9$. Then, the approach proposed in Section 5 ensures that the set $\mathbb{Z} = 3\mathbb{P}$ ($\alpha = 3$) is N-RPI with a maximal number $M = 4$ of attacks over an $N = 10$ steps horizon. Algorithm 1 runs in 0.45 seconds on a *i5-5200U CPU*. To illustrate the use of the obtained N-RPI set, a simulation was done using the attack scenario reported in Fig. 3.

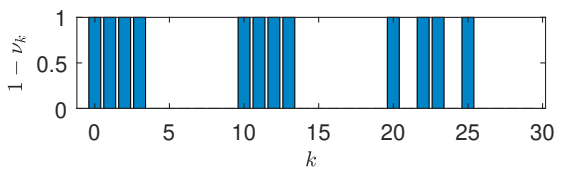

Fig. 3. DoS attack sequence for 30 times. The blue area denotes the DoS activation times

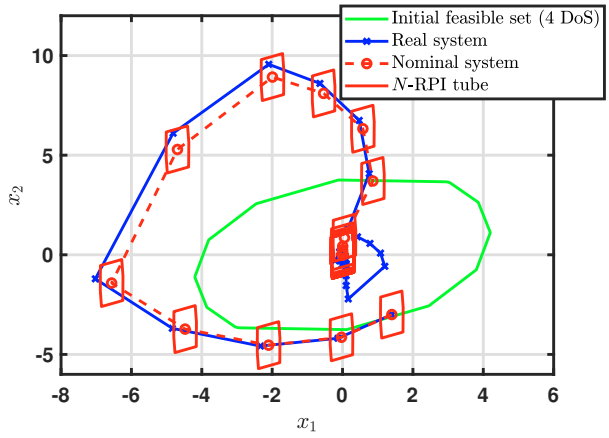

Fig. 4. Tube trajectory of the closed-loop system

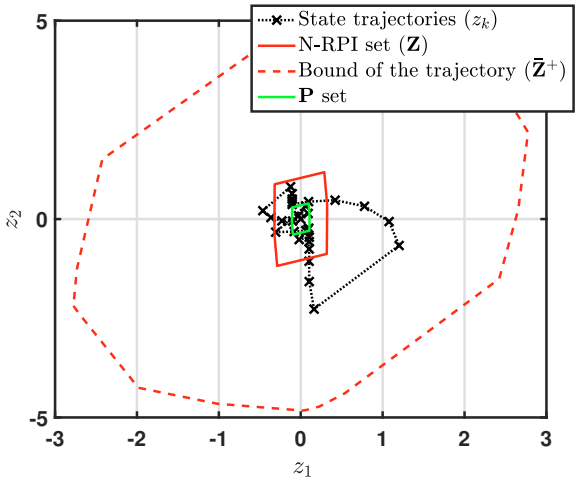

Fig. 5. Trajectory of the difference between the disturbed and the nominal system.

To implement the MPC controller, S is computed as a solution of the Lyapunov equation (13). This results in $S = \begin{bmatrix} 2.2567 & -0.6841 \\ -0.6841 & 1.4846 \end{bmatrix}$. The terminal set is designed as an ellipsoid $\mathbb{X}_f = \{x \in \mathbb{R}^2 \mid ||x||_S^2 < \beta\}$ where $\beta = 0.926$ was computed to obtain the biggest set possible while verifying the assumption 3. Set computations were done using the CORA toolbox (Althoff et al. (2021)), using zonotope to obtain an RPI and then polytopes for the constraints of the MPC problem. The terminal set was inner-approximated by a polytope for convenience of the MPC implementation.

The online MPC problem (8) is formulated as a quadratic programming problem and solved using the function *mp-*

cActiveSetSolver.m provided in the Model Predictive Control Toolbox of Matlab. Starting from an initial state $x_0 = [1.4\ -3]^\top$, Fig. 4 shows the tube trajectory of the system along with the initial feasible set. To better observe the resilient set, Fig. 5 shows the trajectory of the difference z_k, as well as the sets $\mathbb{Z}$, $\bar{\mathbb{Z}}^+$ and $\mathbb{P}$.

7. CONCLUSION

A new resilient and robust control scheme is proposed for a class of CPS subject to state and input constraints, unknown but bounded disturbances and possibly repeated time-limited Denial of Service (DoS) attacks cutting an acknowledgement-based communication between the controller and smart [2] actuators. The proposed tube-based MPC scheme was proved to be robust to unknown-but-bounded disturbances and *jointly* resilient to the DoS attacks. To achieve this, a new robust and resilient invariant set, namely μ-RPI set, was introduced in this paper. Finally, an algorithm was proposed to analyze and evaluate the maximal number M of sample DoS attacks over the MPC time horizon N such that the property of μ-step resilience is still robustly ensured.

This work paves the way for further investigations. In particular, other common attacks such as false data injection or replay attacks may also be considered. Moreover, the original μ-RPI set introduced in this paper is not specific to an MPC context and may be adapted to other control framework. Special attention may be paid on combining μ-RPI sets with other resilient metrics such as the critical time recently proposed in Perodou et al. (2021), all put together to move toward a robust and resilient control of cyber-physical systems.

ACKNOWLEDGEMENTS

This study has been carried out with financial support from the French National Research Agency (ANR) in the framework of the Investments for the Future, Programme IdEx Bordeaux—SysNum (ANR-10-IDEX-03-02). The financial support from the "Région Nouvelle-Aquitaine" is also gratefully acknowledged.

REFERENCES

Allgöwer, F., de Sousa, J.B., Kapinski, J., Mosterman, P., Oehlerking, J., Panciatici, P., Prandini, M., Rajhans, A., Tabuada, P., and Wenzelburger, P. (2019). Position paper on the challenges posed by modern applications to cyber-physical systems theory. *Nonlinear Analysis: Hybrid Systems*, 34, 147–165.

Althoff, M., Kochdumper, N., and Wetzlinger, M. (2021). Cora 2021 manual. *TU Munich*, 85748.

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

Combastel, C. (2003). A state bounding observer based on zonotopes. In *European Control Conference (ECC)*. Cambridge (UK).

Combastel, C. (2015). Zonotopes and Kalman observers: Gain optimality under distinct uncertainty paradigms and robust convergence. *Automatica*, 55, 265–273.

De Persis, C. and Tesi, P. (2015). Input-to-state stabilizing control under denial-of-service. *IEEE Transactions on Automatic Control*, 60(11), 2930–2944.

Franze, G., Lucia, W., and Tedesco, F. (2021). Resilient model predictive control for constrained cyber-physical systems subject to severe attacks on the communication channels. *IEEE Transactions on Automatic Control*, 1–1. doi:10.1109/TAC.2021.3084237.

Gupta, A., Langbort, C., and Başar, T. (2016). Dynamic games with asymmetric information and resource constrained players with applications to security of cyber-physical systems. *IEEE Transactions on Control of Network Systems*, 4(1), 71–81.

Ji, Z., Yang, S., jia Cao, Y., Wang, Y., Zhou, C., Yue, L., and Zhang, Y. (2021). Harmonizing safety and security risk analysis and prevention in cyber-physical systems. *Process Safety and Environmental Protection*, 148, 1279–1291.

Kulmburg, A. and Althoff, M. (2021). On the co-NP-completeness of the zonotope containment problem. *European Journal of Control*, 62, 84–91.

Kumar, S. and Rai, S. (2012). Survey on transport layer protocols: TCP & UDP. *International Journal of Computer Applications*, 46(7), 20–25.

Le, V.T.H., Stoica, C., Dumur, D., Alamo, T., and Camacho, E.F. (2011). Robust tube-based constrained predictive control via zonotopic set-membership estimation. In *2011 50th IEEE Conference on Decision and Control and European Control Conference*, 4580–4585. IEEE.

Lee, E.A. (2015). The past, present and future of cyber-physical systems: A focus on models. *Sensors*, 15(3), 4837–4869.

Marsaglia, G. (1972). Choosing a point from the surface of a sphere. *The Annals of Mathematical Statistics*, 43(2), 645–646.

Mayne, D.Q., Raković, S.V., Findeisen, R., and Allgöwer, F. (2006). Robust output feedback model predictive control of constrained linear systems. *Automatica*, 42(7), 1217–1222.

Perodou, A., Combastel, C., and Zolghadri, A. (2021). Critical-time analysis of cyber-physical systems subject to actuator attacks and faults. *IEEE Conference on Decision and Control (CDC)*.

Poovendran, R., Sampigethaya, K., Gupta, S.K.S., Lee, I., Prasad, K.V., Corman, D., and Paunicka, J.L. (2011). Special issue on cyber-physical systems [scanning the issue]. *Proceedings of the IEEE*, 100(1), 6–12.

Rakovic, S.V., Kerrigan, E.C., Kouramas, K.I., and Mayne, D.Q. (2005). Invariant approximations of the minimal robust positively invariant set. *IEEE Transactions on Automatic Control*, 50(3), 406–410.

Rawlings, J. and Mayne, D. (2009). *Model Predictive Control Theory and Design*. Nob Hill Publishing, Madison, WI.

Sun, Q., Zhang, K., and Shi, Y. (2019). Resilient model predictive control of cyber–physical systems under DoS attacks. *IEEE Transactions on Industrial Informatics*, 16(7), 4920–4927.

[2] here, smart mainly refers to the ability to store a control sequence.