Dual-Rate Control Framework With Safe Watermarking Against Deception Attacks

Iury Bessa, Carlos Trapiello, Vicenç Puig, and Reinaldo Martínez Palhares, *Member, IEEE*

***Abstract*—This article presents a novel secure-control framework against sensor deception attacks. The vulnerability of cyber-physical systems with respect to sensor deceptive attacks makes that all sensor measurements are not reliable until the system security is assured by an attack detection module. Most of the active attack detection strategies require some time to assess the system security, while injecting a watermark signal to ease the detection. However, the injection of watermark signals deteriorates the performance and stability of the plant. The proposed control framework consists of a dual-rate control (DRC) that is able to stabilize the plant using: 1) a model predictive controller that operates at a slower sampling time; 2) a state-feedback predictor-based controller that operates in the nominal sampling time disregarding the use of the untrustworthy measurements until the attack detector is able to certify the security; and 3) a reconfiguration block (RB) for palliating the effect of the watermarking. Simulation results indicate the efficacy of the proposed DRC framework to defend the system from cyber-attacks and the ability of the RB to improve the closed-loop performance during the watermark injection.**

***Index Terms*—Deception attacks, dual-rate control (DRC), model predictive control, predictor-based control, reconfiguration block (RB), secure control, watermark signal.**

I. Introduction

CYBER-PHYSICAL systems (CPSs) appear from the integration between embedded software and physical processes by means of powerful network and communication technologies, under the so-called Internet of Things (IoT) paradigm. On this subject, the development of CPSs raises new concerns regarding safety and security of control systems, such as the avoidance and resilience with respect to cyber attacks.

Cyber attacks are generically classified into denial-of-service (DoS) [1], [2] and deception attacks [3], [4]. On the one hand, DoS attacks affect the transmission channels blocking the communication between the CPS components. On the other hand, deception attacks aim at disrupting the plant operation by injecting false data into some components, such as the controllers or actuators. While the systems are becoming more and more dependent on communication networks, they are also becoming vulnerable to cyber attacks. The existence of such vulnerabilities motivates the study of techniques for cyber-attack detection and secure control with various applications, e.g., electric power systems [5], [6], microgrids [7], water networks [8], mobile robots [9], and transportation systems [10]. The classification of cyber attacks as well as the main methodologies for detection and secure control are revised in [11]–[13].

In particular, this article focuses on secure control against deception attacks, which, while attracting growing interest, is still in an early stage. On this subject, most approaches for mitigating deception attacks are based on the assumption that some sensors/actuators are not compromised (sparse attacks) [14]–[16], in exploiting the analytical redundancy obtained in the context of distributed systems [4], [7], [17], [18] or in the use of stochastic models with known distribution parameters for modeling the attacks [19]–[22]. Whereas the above approaches are efficient under the proposed assumptions, the real attacker behavior may be incompatible with those attack models and/or the safe redundancy may be unavailable.

Chen *et al.* [23] proposed a secure control architecture that integrates machine learning-based attack detectors with a two-layer controller scheme, where a lower tier layer feedback controller that cannot be compromised ensures the stability of the system; and an upper tier layer model predictive controller (MPC) is used to improve the overall performance. Note that switching between different control modes has already been used as an alternative to control linear and nonlinear systems [24], [25]. In particular, Chen *et al.* [25] proposed an MPC-based secure-control strategy that switches between open- and closed-loop control depending on the network security, which is certified by a machine learning-based attack detector designed to ensure the safety of system trajectories.

Manuscript received 2 July 2021; revised 22 November 2021; accepted 6 March 2022. Date of publication 29 March 2022; date of current version 18 November 2022. This work was supported in part by the Brazilian agencies CNPq under Grant 307933/2018-0 and Grant 201370/2019-0; in part by FAPEMIG under Grant PPM-00053-17; in part by PROPG-CAPES/FAPEAM Scholarship Program under Grant 88887.217045/2018-0; in part by the Margarita Salas grant from the Spanish Ministry of Universities; in part by the Spanish State Research Agency (AEI); and in part by the European Regional Development Fund (ERFD) through the Project SaCoAV under Grant MINECO PID2020-114244RB-I00. This article was recommended by Associate Editor Q. Wei. *(Corresponding author: Reinaldo Martínez Palhares.)*

Iury Bessa is with the Department of Electricity, Federal University of Amazonas, Manaus 69067-005, Brazil, and also with the Graduate Program in Electrical Engineering, Federal University of Minas Gerais, Belo Horizonte 31270-901, Brazil (e-mail: iurybessa@ufam.edu.br).

Carlos Trapiello is with Univ. Bordeaux, CNRS, IMS, UMR 5218, 33405 Talence, France (e-mail: carlos.trapiello@u-bordeaux.fr).

Vicenç Puig is with the Institut de Robòtica i Informàtica Industrial, CSIC-UPC, Universitat Politècnica de Catalunya-BarcelonaTech, 08034 Barcelona, Spain (e-mail: vicenc.puig@upc.edu).

Reinaldo Martínez Palhares is with the Department of Electronics Engineering, Federal University of Minas Gerais, Belo Horizonte 31270-901, Brazil (e-mail: rpalhares@ufmg.br).

The performance of the secure control schemes against deception attacks depends on accurate attack detection and modeling. On this subject, a growing body of work has investigated the design of efficient active detection methods. In particular, motivated by its ease of implementation and mild assumptions on the attacker's access to resources, physical watermarking schemes, where an exogenous signal is injected to reveal different types of stealthy attacks, has been thoroughly studied [16], [26]–[28]. However, watermark signals are often devised disregarding the system stability after the attack occurrence. This coupling between secure control schemes and watermarking techniques has been rarely studied, with the exception of [29] where a set-theoretic controller is designed considering the injection of a packet drop watermarking strategy. Similarly, most of the research rely on attack models, which are rarely true.

The literature review indicates two relevant gaps in the design of secure control schemes: 1) dependence on accurate attack modeling, which are often unrealistic since the attacker aims to be stealthy and 2) the inability to account for the effects of the active attack detection systems in the control performance. Motivated by those problems, this work proposes a two-layer cyber-defense strategy against deception attacks affecting the sensors-to-controller channel. The proposed architecture is based on a dual-rate control (DRC) framework where: 1) the lower tier layer works with faster sampling period, and consists of a predictor-based $\mathcal{H}_\infty$ state-feedback controller fed by a state predictor that receives reliable measurements at each T samples and 2) the upper tier is a robust MPC that works with slower sampling period and is updated only when a new reliable measurement arrives. Consequently, the attack resilience is attained by operating in an open-loop fashion in the time between reliable measurements (i.e., disregarding possible untrustworthy measurements). The secure operation offers a time window to certificate the reliability of the data through the injection of a watermark signal. A generic user-defined watermarking strategy has been modeled using an unknown-but-bounded signal description. On the other hand, the secure operation attained by means of the intermittent measurement behavior of the DRC comes at the price of increasing the sensitivity to uncertainties (among which is the watermark signal) compared to a standard controller operating at the higher sampling rate. In order to attenuate these deteriorating effects, the DRC framework is complemented with the design of a dynamic reconfiguration block (RB), which aims at hiding the effects of the watermark signal from the controller.

Notice that multirate control techniques have been already employed in networked control systems to avoid package disorder and reduce the network usage [30], [31], as well as in distributed systems where the subsystems operate at different time scales [32]. In addition, a cyber-attack detection approach is introduced in [33] by using multirate control to ensure minimum-phase dynamics. The proposed DRC framework resembles those proposed in [23] and [25], which present two-layer control frameworks with lower tier explicit feedback controllers and upper tier MPCs, and consider the effect of the integration between the attack detector and the control system. Besides, in [25], the open-loop control mode is adopted while the sensor measurements are not reliable. However, the proposed DRC framework addresses two issues ignored by [23] and [25]: 1) it considers the effect of an active attack detection with watermarking by employing the RB to reduce them, while the papers [23] and [25] propose the integration with a passive attack detectors and 2) it is robust with respect to additive disturbance, which motivates the use of the tube-based MPC in the upper tier layer, otherwise, [23] and [25] consider the MPC of systems without uncertainties.

The RBs are usually employed in fault-tolerant control based on fault hiding [34]–[36]. The key idea of this technique is the insertion of a block to hide the fault effects from the controller and plant disregarding controller redesign. The most common structures of RBs are the virtual actuators (VAs) and virtual sensors for faults in actuators and sensors, respectively, [37]. Within the cyber-security context, VAs are used in [1] to deal with DoS attacks that are modeled as an actuator efficiency loss, and in [38] for masking the effects of the watermarking signal from the controller. In this article, a novel RB structure is proposed for minimizing the effect of the watermarking in a dual-rate predictive control scheme. Notice that the RB fits well to the control framework proposed in this article, since the ability of hiding the fault effect can be extended to hide watermarking signal.

According to the stated above, the main contributions of this article are summarized as follows.

1) A novel DRC strategy is used as defense against sensor deception attacks; the controller maintains the plant stability until a reliable measurement is observed, i.e., after a watermarking-based certification.
2) The controller has two layers: the first one (faster) is the predictor-based $\mathcal{H}_\infty$ state-feedback controller that stabilizes the closed-loop system based on predictions of the system output while the measurements are not reliable; and the second layer (with a slower sampling period than the first one) is an MPC controller that ensures the compliance with input and state constraints.
3) An RB is used to improve the DRC's performance by providing a guaranteed $\mathcal{H}_\infty$-norm with respect to the watermark signal used for detecting attacks.

The remainder of this article is organized as follows. Section II provides an overview of the proposed solution. Section III describes the design of the state-feedback gain used for the lower layer. Section IV presents the RB design. Section V presents the MPC design used in the upper layer. Section VI evaluates the proposed DRC by means of simulations. Finally, Section VII draws the conclusions.

Notation: The following notations are used in this work. $\mathbb{R}^n$, $\mathbb{N}$, and $\mathbb{N}_{\leq i}$ denote, respectively, the n-dimensional Euclidean space, the set of non-negative integer numbers, and the set of non-negative integers less than or equal to $i \in \mathbb{N}$. For a matrix X, $X \succ (\prec)\ 0$ means that X is positive (negative) definite; $X^\top$ denotes its transpose; $X^\dagger$ denotes its Moore–Penrose pseudoinverse. For a symmetric $P \succ 0$, $\|x\|_P \triangleq x^\top P x$. The identity matrix of dimension n is denoted by I_n and the null matrix of order $n \times m$ by $0_{n\times m}$. In a symmetric block matrix, "$\star$" is the term deduced by symmetry; $\text{diag}\{d_1, \ldots, d_n\}$ is a diagonal matrix with the elements/blocks $d_1, \ldots, d_n$ in the

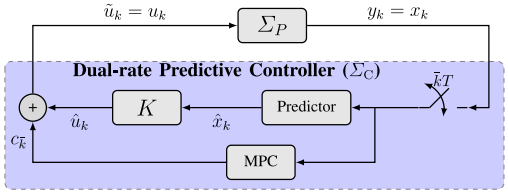

Fig. 1. Secure operation.

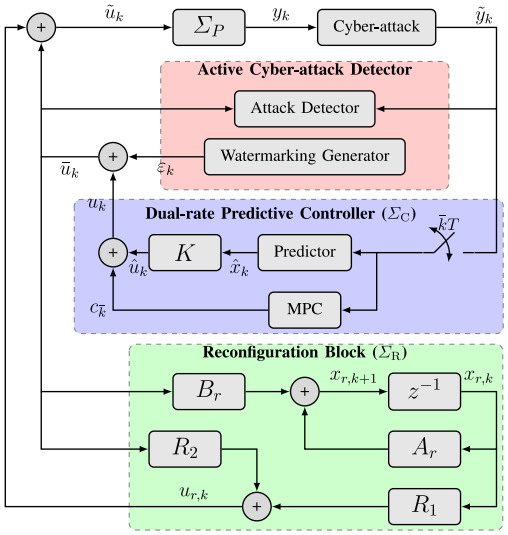

Fig. 2. Detection operation.

main diagonal. The Minkowski sum and the Pontryagin difference of two sets $\mathcal{X}$ and $\mathcal{Y}$ are defined, respectively, by $\mathcal{X} \oplus \mathcal{Y} \triangleq \{x+y | x \in \mathcal{X}, y \in \mathcal{Y}\}$ and $\mathcal{X} \ominus \mathcal{Y} \triangleq \{x | x \oplus \mathcal{Y} \subseteq \mathcal{X}\}$. The integer remainder operation between $a \in \mathbb{N}$ and $b \in \mathbb{N}_{\geq 1}$ is denoted by $a\%b$.

II. Preliminaries

A. Proposal Overview

To investigate the secure control of a dynamic system subject to sensor deception attacks, two operation modes are considered: 1) secure operation and 2) detection operation.

The secure operation, illustrated in Fig. 1, occurs when the measurements are assumed to be reliable, (i.e., a cyber-attack detector system already tested and ensured that it is not occurring a cyber attack). In this case, a dual-rate controller Σ_C with two layers is employed for ensuring the stability of the plant Σ_P. The lower layer is an $\mathcal{H}_\infty$ state-feedback controller K, which is designed to work on the nominal sample rate, and the upper layer is a robust MPC controller. However, the output channel is read only at each T samples to defend the controller from cyber attacks that can appear after the security certification. Accordingly, the $\mathcal{H}_\infty$ state-feedback controller is fed by a state predictor that is refreshed at each T samples.

The detection operation mode, depicted in Fig. 2, occurs between two reliable samples obtained with a slower sample time T. Notice that only the output measurement y_k is transmitted through the network and it may be subject to cyber attacks. In that mode, a watermark signal is injected in the system while an attack detection module evaluates the plant inputs and outputs to check the measurements' reliability. In addition, an RB is inserted to improve the DRC performance.

Hereafter, the systems under consideration are described by the following discrete-time linear time-invariant model:

$$\Sigma_P : \begin{cases} x_{k+1} = Ax_k + B\tilde{u}_k + Ew_k \\ z_k = Cx_k + D\tilde{u}_k + Fw_k \\ y_k = I_n x_k \end{cases} \tag{1}$$

where A, B, C, D, E, and F are the state-space matrices with adequate dimensions, $x_k \in \mathcal{X} \subset \mathbb{R}^n$ is the state vector at the time instant k, $\tilde{u}_k \in \tilde{\mathcal{U}} \subset \mathbb{R}^m$ is the input vector, $z_k \in \mathcal{Z} \subset \mathbb{R}^p$ is a performance output, $y_k \in \mathbb{R}^n$ is the state measurements, and $w_k \in \mathcal{W} \subset \mathbb{R}^q$ is an exogenous disturbance described as

$$\mathcal{W} = \left\{ w \in \mathbb{R}^n | w^\top w \leq \kappa \right\}. \tag{2}$$

The plant input signal $\tilde{u}_k$ presents three components

$$\tilde{u}_k = u_k + u_{r,k} + \varepsilon_k \tag{3}$$

where u_k is the control signal computed by dual-rate controller, $\varepsilon_k \in \mathcal{E} \subset \mathbb{R}^m$ is the watermarking signal used for attack detection, and $u_{r,k} \in \mathbb{R}^m$ is the RB signal. This RB signal will be designed to satisfy (cf. Section IV)

$$\bar{u}_{r,k} = u_{r,k} + \varepsilon_k \tag{4}$$

$$\bar{u}_{r,k} \in \mathcal{R} \tag{5}$$

where $\mathcal{R}$ is a partition of the input constraint set reserved to the watermarking and RB signals.

In the proposed framework, during the secure operation $\varepsilon_k = 0$ and $u_{r,k} = 0$, and therefore, $\tilde{u}_k = u_k$ as shown in Fig. 1. The other components are added only in the detection operation as depicted in Fig. 2. Consequently, the MPC action should be designed for ensuring the state and input constraints.

B. Attack Model

In this article, it is assumed that a malicious attacker is able to access and corrupt the (possible watermarked) measurement in sensor-to-controller channel in order to disrupt the system's operation while remaining undetected. Accordingly, denoting the measurements signal received at the controller's side of the network as $\tilde{y}_k \in \mathbb{R}^n$, then

$$\tilde{y}_k = \begin{cases} \phi\left(\boldsymbol{y}_{k-N'-1:k}\right), & \text{attack} \\ y_k, & \text{otherwise} \end{cases} \tag{6}$$

where $\boldsymbol{y}_{k-N'-1:k} = \{y_{k-N'-1}, \ldots, y_k\}$ is a sequence of the last N' measurement values and $\phi : \mathbb{R}^n \times \mathbb{R}^{N'} \to \mathbb{R}^n$ is a mapping describing the attacker's policy [39].

Remark 1: Notice that since the proposed approach does not rely on some specific model of deception attack, (6) represents a generic attack model. This representation encompasses a wide variety of deception attacks, including: false-data injection attacks $\tilde{y}_k = y_k + a_k$, where a_k describes malicious data added to the measurements; replay attacks $\tilde{y}_k = y_{k-T_a}$, where T_a denotes the time shift induced by the attack, or rerouting attacks $\tilde{y}_k = Ry_k$, where R is a routing matrix [40].

C. Secure Operation

In this section, the proposed DRC is discussed. DRC computes the signal u_k that is the only signal injected in the plant during the secure operation, i.e., $\tilde{u}_k = u_k$. The control signal u_k has two components: 1) an $\mathcal{H}_\infty$ state-feedback action $\hat{u}_k$, which is fed by a state predictor that obtains the correct state measurement at each T samples and 2) a finite horizon MPC action $c_{\bar{k}}$, which is updated at each T samples. Accordingly, considering that the controller receives a real (reliable) measurement at $k = 0$, it results that

$$u_k = \hat{u}_k + c_{\bar{k}} \tag{7}$$

where $\bar{k} \in \mathbb{N}$ denotes the ordinality of the real measurement samples, i.e., a new real measurement is sampled at each instant $k = \bar{k}T$. It follows that:

$$\hat{u}_k = \begin{cases} Kx_k, & \text{if } k = \bar{k}T \\ K\hat{x}_k, & \text{if } k \neq \bar{k}T. \end{cases} \tag{8}$$

Assumption 1: Under secure conditions, the correct value of the system states is provided at each T samples, i.e., $\hat{x}_{\bar{k}T+1} = Ax_{\bar{k}T} + Bu_{\bar{k}T}$ and $u_{\bar{k}T} = Kx_{\bar{k}T} + c_{\bar{k}}$ for all $\bar{k} \in \mathbb{N}$.

The control signal in (7) is based on Assumption 1 and depends on the predictions generated by the following predictor:

$$\hat{x}_{k+1} = \begin{cases} Ax_k + Bu_k, & \text{if } k = \bar{k}T \\ A\hat{x}_k + Bu_k, & \text{if } k \neq \bar{k}T \end{cases} \tag{9}$$

where $\hat{x}_k \in \mathbb{R}^n$ is the prediction of x_k and $\hat{x}_0 = x_0$.

The state-feedback gain K should be designed to ensure the stability of the closed-loop system with guaranteed performance with respect to the prediction error $v_k = \hat{x}_k - x_k$. Otherwise, the MPC action is designed to ensure reference tracking and also that the system state remains within the domain of attraction of the local state-feedback controller.

Remark 2: Assumption 1 indicates that the design of the proposed DRC framework requires accurate measurements of the states at each T samples. In this regard, the data integrity checking is carried out in the detection operation presented in Section II-D. Thus, it is expected that some measurement noises or estimation errors appear in the measurement of $x_{\bar{k}T}$ that is used to refresh the predictor and design the MPC.

D. Detection Operation

In the detection operation, the watermark signal ε_k is injected for detecting the deception attack occurrence. It starts periodically at the beginning of each T cycle, i.e., at $k = nT$.

Assumption 2: There exists a detector that is able to detect the cyber-attack occurrence. Assume that the maximum time spent for detecting an attack is $T_d \in \mathbb{N}$ and the time required for countermeasures against an attack is $T_r \in \mathbb{N}$, such that $T_d + T_r \leq T$.

Remark 3: Note that the attack detectability is enhanced by means of a user's defined watermark signal characterized following an unknown-but-bounded description using the set $\mathcal{E}$. On the other hand, the achievement of reliable measurements after detection can be addressed by refreshing the communication medium (software rejuvenation [41]).

During the detection operation, the control strategy described in Section II-C is maintained, but an RB is inserted in the loop to hide the effect of the watermark signal injection from the controllers' signals. The design of the attack detector and watermark signal is out of the scope of this article, however, the RB design is based on the following assumption on the set $\mathcal{E}$:

$$\mathcal{E} = \left\{ \varepsilon \in \mathbb{R}^m | \varepsilon^\top \varepsilon \leq \delta \right\}. \tag{10}$$

Remark 4: The use of watermark signals has been proposed to detect cyber attacks [16], [27], [39]. The watermarking signals are generally i.i.d. Gaussian random variables [16], but they can also be optimized to increase the attack detectability [27], or generated by watermarking filters [39].

The RB Σ_R, which is described below, is inserted in the loop to compensate for the effects of ε_k by hiding its effects from the controller but not from the detector. Such approach allows to preserve the stability of the system under attack during the watermarking signal injection phase. The RB is described as follows:

$$\Sigma_R : \begin{cases} x_{r,k+1} = A_r x_{r,k} + B_r \bar{u}_k \\ u_{r,k} = R_1 x_{r,k} + R_2 \bar{u}_k \end{cases} \tag{11}$$

where $x_{r,k} \in \mathbb{R}^n$ is the vector of states of the RB, $u_{r,k}$ is the reconfiguration signal, which compensates for the watermarking effects, and $\bar{u}_k$ is

$$\bar{u}_k = u_k + \varepsilon_k. \tag{12}$$

The signal $u_{r,k}$ is added to the input u_k to mitigate the harmful effects of the watermarking signal ε_k, such that the resulting input $\tilde{u}_k$, considering the controller and the RB signals, is described (cf. Fig. 2) as follows:

$$\tilde{u}_k = \bar{u}_k + u_{r,k}. \tag{13}$$

Both the $\mathcal{H}_\infty$ controller and the MPC can be designed despite of the watermarking and RB effect, thanks to (5).

E. Problem Statement

Based on the above discussion, this article addresses the problem of designing a control framework to guarantee the plant stability despite the occurrence of sensor deception attacks without assumptions about the attack signals. For this purpose, we only assume that there exists an active attack detection system, which is able to periodically certify the security of the measurements. Thus, the proposed defense strategy is based on the use of only secure samples certified by the attack detector. However, it is well-known the disruptive effect of active attack detection system due to the signal injection. In particular, this effect is exacerbated when the measurements cannot be read every time due to the defense strategy. In this sense, the second problem addressed by this work is to design an RB, which is able to attenuate the undesired effects of the watermarking without losing the residual generation ability. Accordingly, the problems addressed in this article can be stated as follows.

Problem 1: Consider the plant Σ_P represented by (1) with $w_k \in \mathcal{W}$ and the DRC framework depicted in Fig. 1 based

on the predictor (9) subject to Assumptions 1 and 2. Find the gain K and the MPC action $c_{\bar{k}}$, which ensure that Σ_P is robustly stable with respect the prediction error during the secure operation and the constraints $x_k \in \mathcal{X}$ and $\tilde{u}_k \in \tilde{\mathcal{U}}$ hold.

Problem 2: Consider the plant Σ_P represented by (1) with $w_k \in \mathcal{W}$ and the DRC framework depicted in Fig. 2 based on the predictor (9) subject to Assumptions 1 and 2 and to the watermark signal $\varepsilon_k \in \mathcal{E}$. Find the RB Σ_R in (11), which minimizes the performance degradation due to ε_k.

III. Design of the $\mathcal{H}_\infty$ State-Feedback Controller

The feedback of the predictions of the states produces an additional disturbance $v_k \in \mathbb{R}^n$ in the control input channel. The $\mathcal{H}_\infty$ predictor-based controller described by (8) and (9) is represented by the following simplified law:

$$\hat{u}_k = Kx_k + Kv_k \tag{14}$$

where recalling that at each T samples the predictor is refreshed with reliable data, the error v_k induced by the state predictor (9) can be bounded as $\|v_k\| \leq \bar{v}$ (cf. Section V-A). Therefore, neglecting the effects of the MPC action $c_{\bar{k}}$ and the watermarking signal ε_k, and considering the above simplified state-feedback law, the inner control loop is represented as

$$\begin{cases} x_{k+1} = \bar{A}x_k + \bar{B}\bar{w}_k \\ z_k = \bar{C}x_k + \bar{D}\bar{w}_k \\ y_k = I_n x_k \end{cases} \tag{15}$$

where $\bar{w}_k = [v_k^\top \ w_k^\top]^\top$, $\bar{A} = A + BK$, $\bar{C} = C + DK$, $\bar{B} = [BK \ E]$, and $\bar{D} = [DK \ F]$.

The noise sensitivity transfer function $T_{\bar{w}z} : \bar{w} \mapsto z$ is nonexpansive if and only if $\Sigma_{k=0}^{\infty} z_k^\top z_k \leq \Sigma_{k=0}^{\infty} \bar{w}_k^\top \bar{w}_k$. Thus, the $\mathcal{H}_\infty$-norm is $\|T_{\bar{w}z}\|_\infty \leq \gamma$, if the performance index $\mathcal{I}_\infty = \sum_{k=0}^{\infty} z_k^\top z_k - \gamma^2 \bar{w}_k^\top \bar{w}_k$ is negative. In this case, (15) is said robustly stable with $\|T_{\bar{w}z}\|_\infty \leq \gamma$.

Theorem 1: The control law (14) ensures the robust stability of (15) with guaranteed $\mathcal{H}_\infty$-norm $\|T_{\bar{w}z}\|_\infty \leq \gamma$ if the following condition holds:

$$\begin{bmatrix} P - V - V^\top & \star & \star & \star & \star \\ 0_{n\times n} & \rho I_n - V - V^\top & \star & \star & \star \\ 0_{q\times n} & 0_{q\times n} & -\rho I_q & \star & \star \\ AV + BY & BY & \rho E & -P & \star \\ CV + DY & DY & \rho F & 0_{n\times n} & -I_n \end{bmatrix} \prec 0 \tag{16}$$

for some matrices $P \succ 0$, Y, V, and scalar $\rho > 0$. The gain K and guaranteed norm ρ are given, respectively, by

$$K = YV^{-1}, \quad \gamma = \rho^{\frac{1}{2}}. \tag{17}$$

Proof: Choose the following Lyapunov candidate function $V(x_k) = x_k^\top P^{-1} x_k$ with $P \succ 0$. The difference $\Delta V(x_k) = V(x_{k+1}) - V(x_k)$ is given by

$$\Delta V(x_k) = \left(\bar{A}x_k + \bar{B}\bar{w}_k\right)^\top P^{-1}\left(\bar{A}x_k + \bar{B}\bar{w}_k\right) - x_k^\top P^{-1} x_k$$

which can be represented in matrix form as

$$\begin{bmatrix} x_k \\ \bar{w}_k \end{bmatrix}^\top \begin{bmatrix} \bar{A}^\top P^{-1}\bar{A} - P^{-1} & \star \\ \bar{B}^\top P^{-1}\bar{A} & \bar{B}^\top P^{-1}\bar{B} \end{bmatrix} \begin{bmatrix} x_k \\ \bar{w}_k \end{bmatrix} \prec 0. \tag{18}$$

Given Young's inequalities $\rho I_n - V^\top - V \succeq -\rho^{-1} V^\top V$ and $P - V^\top - V \succeq -V^\top P^{-1} V$, thus (16) implies

$$\begin{bmatrix} -V^\top P^{-1} V & \star & \star & \star & \star \\ 0_{n\times n} & -\rho^{-1} V^\top V & \star & \star & \star \\ 0_{q\times n} & 0_{q\times n} & -\rho I_q & \star & \star \\ AV + BY & BY & \rho E & -P & \star \\ CV + DY & DY & \rho F & 0_{n\times n} & -I_n \end{bmatrix} \prec 0$$

that is equivalent to the following inequality, considering (17), when it is post and premultiplied, respectively, by $\mathrm{diag}\left\{V^{-1}, V^{-1}, \rho^{-1} I_q, I_n, I_n\right\}$ and its transpose

$$\begin{bmatrix} -P^{-1} & \star & \star & \star & \star \\ 0_{n\times n} & -\rho^{-1} I_n & \star & \star & \star \\ 0_{q\times n} & 0_{q\times n} & -\rho^{-1} I_q & \star & \star \\ A + BK & BK & E & -P & \star \\ C + DK & DK & F & 0_{n\times n} & -I_n \end{bmatrix} \prec 0.$$

According to Schur's complement lemma and substituting (17), it follows that (16) is equivalent to

$$\begin{bmatrix} \bar{A}^\top P \bar{A} - P + \bar{C}^\top \bar{C} & \star \\ \bar{B}^\top P \bar{A} + \bar{D}^\top \bar{C} & \bar{B}^\top P \bar{B} + \bar{D}^\top \bar{D} - \gamma^2 I_n \end{bmatrix} \prec 0. \tag{19}$$

Pre and postmultiplying (19), respectively, by $[x_k^\top \ \bar{w}_k^\top]$ and its transpose, and considering (18), it follows that:

$$\sum_{k=0}^{\infty} z_k^\top z_k - \gamma^2 \bar{w}_k^\top \bar{w}_k + \Delta V(x_k) < 0. \tag{20}$$

Note that the first element of (19) ensures that (15) is asymptotically stable. If the closed-loop system is asymptotically stable and considering null initial conditions, then $V(x_k)|_{k=0} = V(x_k)|_{k\to\infty} = 0$ and (20) is equivalent to

$$\sum_{k=0}^{\infty} z_k^\top z_k - \gamma^2 \bar{w}_k^\top \bar{w}_k + \Delta V(x_k) - \Delta V(x_k) < 0. \tag{21}$$

Finally, (21) implies $\mathcal{I}_\infty < 0$. Therefore, (15) is robustly stable with the guaranteed $\mathcal{H}_\infty$-norm $\|T_{\bar{w}z}\|_\infty \leq \gamma$. ∎

The state-feedback controller designed by means of Theorem 1 is able to guarantee the $\mathcal{H}_\infty$-norm $\|T_{\bar{w}z}\|_\infty \leq \gamma$. However, during the detection operation, the prediction error v_k and, consequently, $\bar{w}_k$ tends to increase, which also should make z_k increase and x_k diverge from the origin. Although the prediction error is reset at each T samples, it is necessary to ensure that the constraint $x_k \in \mathcal{X}$ always holds. To ensure it, the MPC action c_k is designed in Section V.

IV. Design of the $\mathcal{H}_\infty$ Reconfiguration Block

In the sequel, the RB is designed to make the plant dynamics (1) converge to the nominal system dynamics given by the predictor dynamics (without attack, watermarking, RB, and disturbances). Considering the control signal (7), and the RB in (11), then the plant and predictor states, respectively, x_k and $\hat{x}_k$, are described as follows:

$$x_{k+1} = Ax_k + BR_1 x_{r,k} + B(K + R_2 K)\hat{x}_k + (B + BR_2)\varepsilon_k + Ew_k \tag{22}$$

$$\hat{x}_{k+1} = (A + BK)\hat{x}_k. \tag{23}$$

Let the error signals $x_{\Delta,k}$ and e_k be defined as follows:

$$x_{\Delta,k} = x_{r,k} - \hat{x}_k \tag{24}$$

$$e_k = x_{r,k} - x_k. \tag{25}$$

Therefore, the errors' dynamics are described as follows:

$$\begin{aligned} x_{\Delta,k+1} &= A_r x_{r,k} + B_r K\hat{x}_k + B_r\varepsilon_k - \bar{\Phi}\hat{x}_k \\ &\quad \pm\big(\bar{\Phi} + B_r K\big)x_{r,k} \\ &= \big(\bar{\Phi}_r - \bar{\Phi}\big)x_{r,k} + \big(\bar{\Phi} - B_r K\big)x_{\Delta,k} + B_r\varepsilon_k \qquad (26) \\ e_{k+1} &= A_r x_{r,k} + B_r K\hat{x}_k + B_r\varepsilon_k - \big[Ax_k + BR_1 x_{r,k} \\ &\quad + B(K + R_2 K)\hat{x}_k + (B + BR_2)\varepsilon_k + Ew_k\big] \\ &\quad \pm\big(\bar{\Phi} + BR_2 K + B_r K\big)x_{r,k} \\ &= \big(\bar{\Phi}_r - \bar{\Phi}\big)x_{r,k} + \big(\bar{\Phi} - B_r\big)x_{\Delta,k} \qquad (27) \end{aligned}$$

where $\bar{\Phi} = A + BK$ and $\bar{\Phi}_r = A_r + B_r K$. Similarly, the RB in (11) can be rewritten as

$$\Sigma_R : \begin{cases} x_{r,k+1} = \bar{\Phi}_r x_{r,k} - B_r K x_{\Delta,k} + B_r\varepsilon_k \\ u_{r,k} = (R_1 + R_2 K)x_{r,k} - R_2 K x_{\Delta,k} + R_2\varepsilon_k. \end{cases} \tag{28}$$

Therefore, defining $\tilde{x}_k^\top = [x_{r,k}^\top \;\; x_{\Delta,k}^\top \;\; e_k^\top]$, and $\tilde{w}_k^\top = [\varepsilon_k^\top \;\; w_k^\top]$, the following dynamics are obtained:

$$\begin{aligned} \tilde{x}_{k+1} &= \tilde{A}\tilde{x}_k + \tilde{B}\tilde{w}_k \\ \tilde{z}_k &= \tilde{C}\tilde{x}_k = x_k \end{aligned} \tag{29}$$

where

$$\tilde{A} = \begin{bmatrix} \bar{\Phi}_r & -B_r K & 0 \\ \bar{\Phi}_r - \bar{\Phi} & \bar{\Phi} - B_r K & 0 \\ \bar{\Phi}_r - \bar{\Phi} - B(R_1 + R_2 K) & B_\Delta & A \end{bmatrix}$$

$$\tilde{B}_1 = \begin{bmatrix} B_r \\ B_r \\ B_r - BR_2 - B \end{bmatrix}, \quad \tilde{B}_2 = \begin{bmatrix} 0 \\ 0 \\ -E \end{bmatrix}, \quad \tilde{B} = \begin{bmatrix} \tilde{B}_1 & \tilde{B}_2 \end{bmatrix}$$

$$B_\Delta = BK + BR_2 K - B_r K, \quad \tilde{C} = [I_n \; 0 \; -I_n].$$

The RB input $u_{r,k}$ can be also written as

$$u_{r,k} = \bar{R}\tilde{x}_k + R_2\varepsilon_k \tag{30}$$

where $\bar{R} = \begin{bmatrix} R_1 + R_2 K & -R_2 K & 0 \end{bmatrix}$.

The RB is designed to ensure the robust stability of (29) with guaranteed $\mathcal{H}_\infty$-norm $\|T_{\tilde{w}\tilde{z}}\|_\infty \leq \tilde{\gamma}$.

Theorem 2: The RB Σ_R described in (11) ensures the robust stability of (29) with guaranteed $\mathcal{H}_\infty$-norm $\|T_{\tilde{w}\tilde{z}}\|_\infty \leq \tilde{\gamma}$ if the following condition holds:

$$\begin{bmatrix} -\tilde{V} - \tilde{V}^\top + \tilde{P} & 0 & Y_A & Y_B \\ \star & -I_n & \tilde{C} & 0 \\ \star & \star & -\tilde{P} & 0 \\ \star & \star & \star & -\tilde{\rho} I_{q+m} \end{bmatrix} \prec 0$$

$$Y_A = \tilde{V}\tilde{A} = \begin{bmatrix} \tilde{\Phi}_r & -\tilde{B}_r K & 0 \\ \tilde{\Phi}_r - \tilde{\Phi} & \tilde{\Phi} - \tilde{B}_r K & 0 \\ \tilde{\Phi}_r - \tilde{\Phi} - (\tilde{R}_1 + \tilde{R}_2)K & \tilde{B}_\Delta & V_r A \end{bmatrix}$$

$$Y_B = \tilde{V}\tilde{B} = \begin{bmatrix} \tilde{B}_r & 0 \\ \tilde{B}_r & 0 \\ -B_\Delta & -V_r E \end{bmatrix}$$

$$\tilde{\Phi} = V_r A + V_r BK, \quad \tilde{\Phi}_r = \tilde{A}_r + \tilde{B}_r K$$

$$\tilde{B}_\Delta = V_r BK + \tilde{R}_2 K - \tilde{B}_r K, \quad \tilde{V} = \mathrm{diag}\{V_r, V_r, V_r\} \tag{31}$$

for some matrices $\tilde{P} \succ 0$, A_r, $\tilde{B}_r$, $\tilde{R}_1$, $\tilde{R}_2$, V_r, and scalar $\tilde{\rho} > 0$, and a given state-feedback gain K. The RB matrices and the guaranteed norm $\tilde{\gamma}$ are given by

$$A_r = V_r^{-1}\tilde{A}_r, \quad B_r = V_r^{-1}\tilde{B}_r, \quad R_1 = (V_r B)^\dagger \tilde{R}_1 \tag{32}$$

$$R_2 = (V_r B)^\dagger \tilde{R}_2, \quad \tilde{\gamma} = \sqrt{\tilde{\rho}}. \tag{33}$$

Proof: Choosing $V(\tilde{x}_k) = \tilde{x}_k^\top \tilde{P}\tilde{x}_k$ as the Lyapunov candidate function with a symmetric positive-definite matrix $\tilde{P}$, the difference $\Delta V = V(\tilde{x}_{k+1}) - V(\tilde{x}_k)$ is

$$\Delta V(\tilde{x}_k) = \begin{bmatrix} \tilde{x}_k \\ \tilde{w}_k \end{bmatrix}^\top \begin{bmatrix} \tilde{A}^\top \tilde{P}\tilde{A} - \tilde{P} & \tilde{B}^\top \tilde{P}\tilde{A} \\ \star & \tilde{B}^\top \tilde{P}\tilde{B} \end{bmatrix} \begin{bmatrix} \tilde{x}_k \\ \tilde{w}_k \end{bmatrix}.$$

Let $\mathcal{I}_\infty = \sum_{k=0}^{\infty} \tilde{z}_k^\top \tilde{z}_k - \tilde{\gamma}^2 \tilde{w}_k^\top \tilde{w}_k$ be the performance index. Following the same steps of the proof of Theorem 1, if the closed-loop system is asymptotically stable and considering null initial conditions, then $\mathcal{I}_\infty < 0$, for $V(\tilde{x}_k)|_{k=0} = V(\tilde{x}_k)|_{k\to\infty} = 0$. It holds if

$$\begin{bmatrix} \tilde{C}^\top \tilde{C} + \tilde{A}^\top \tilde{P}\tilde{A} - \tilde{P} & \tilde{B}^\top \tilde{P}\tilde{A} \\ \star & \tilde{B}^\top \tilde{P}\tilde{B} - \tilde{\gamma}^2 I_{n+m} \end{bmatrix} \prec 0. \tag{34}$$

Considering $-\tilde{V} - \tilde{V}^\top + \tilde{P} \succeq -\tilde{V}^\top \tilde{P}^{-1}\tilde{V}$, and (33), then (31) implies

$$\begin{bmatrix} -\tilde{V}^\top \tilde{P}^{-1}\tilde{V} & 0 & Y_A & Y_B \\ \star & -I_n & \tilde{C} & 0 \\ \star & \star & -\tilde{P} & 0 \\ \star & \star & \star & -\tilde{\gamma}^2 I_{q+m} \end{bmatrix} \prec 0. \tag{35}$$

Pre and postmultiplying (35) by, respectively, $\mathrm{diag}\{\tilde{V}^{-\top}, I_n, I_{3n}, I_{q+m}\}$ and its transpose, and considering (32), (33), it implies

$$\begin{bmatrix} -\tilde{P} & 0 & \tilde{A} & \tilde{B} \\ \star & -I_n & \tilde{C} & 0 \\ \star & \star & -\tilde{P} & 0 \\ \star & \star & \star & -\tilde{\gamma}^2 I_{q+m} \end{bmatrix} \prec 0 \tag{36}$$

which results in (34), according to Schur's complement Llemma. Therefore, using the arguments of Theorem 1's proof, it is shown that (31) ensures that (29) is robustly stable with the $\mathcal{H}_\infty$-norm $\|T_{\tilde{w}\tilde{z}}\|_\infty \leq \tilde{\gamma}$. ■

Theorem 3: Let the signal $\bar{u}_{r,k}$ be defined according to (4), for the watermark $\varepsilon_k \in \mathcal{E}$ and the RB signal $u_{r,k}$ [cf. (10) and (30)], and the set $\mathcal{R}$ be

$$\mathcal{R} = \Big\{u \in \mathbb{R}^m | u^\top P_u u \leq 1\Big\}. \tag{37}$$

The inclusion $\bar{u}_{r,k} \in \mathcal{R}$ holds if there exist symmetric positive-definite matrices Q and P_u, and positive scalars σ_2, σ_4, and τ_1, satisfying

$$1 - \sigma_1 - \delta\sigma_2 - \sigma_3 - \kappa\sigma_4 \geq 0 \tag{38}$$

$$1 - \tau_1 - \delta\tau_2 \geq 0 \tag{39}$$

$$\Theta \succeq 0, \qquad \Lambda \preceq 0$$

$$\Theta = \begin{bmatrix} \Theta_{11} & \Theta_{12} & \Theta_{13} \\ \star & \Theta_{22} & \Theta_{23} \\ \star & \star & \Theta_{33} \end{bmatrix}, \quad \Lambda = \begin{bmatrix} \Lambda_{11} - \tau_1 Q & \Lambda_{12} \\ \star & \Lambda_{22} - \tau_2 I_m \end{bmatrix}$$

$$\Theta_{11} = -\tilde{A}^\top Q\tilde{A} + \sigma_1 Q + \sigma_3\Lambda_{11}, \; \Theta_{12} = -\tilde{A}^\top Q\tilde{B}_1 + \sigma_3\Lambda_{12}$$

$$\Theta_{22} = -\tilde{B}_1^\top Q\tilde{B}_1 + \sigma_2 I_m + \sigma_3\Lambda_{22}, \; \Theta_{33} = -\tilde{B}_2^\top Q\tilde{B}_2 + \sigma_4 I_n$$

$$\Theta_{23} = -\tilde{B}_1^\top Q \tilde{B}_2,\ \ \Lambda_{22} = (R_2 + I_m)^\top P_u (R_2 + I_m)$$
$$\Lambda_{11} = \bar{R}^\top P_u \bar{R},\ \ \Lambda_{12} = \bar{R}^\top P_u (R_2 + I_m) \tag{40}$$

for given positive scalars σ_1, σ_3, and τ_2.

Proof: Based on (30) and (37), for $\xi_k^\top = [\tilde{x}_k^\top \ \varepsilon_k^\top]$ and $G = [\bar{R}\ R_2 + I_m]$, the inclusion $\varepsilon_k + u_{r,k} \in \mathcal{R}$ results

$$\xi_k^\top G^\top P_u G \xi_k \leq 1. \tag{41}$$

Using the S-procedure, and considering that $\varepsilon_k \in \mathcal{E}$ and $w_k \in \mathcal{W}$, with $\mathcal{E}$ and $\mathcal{W}$ described, respectively, in (10) and (2), the following inequality implies (41):

$$\Big(1 - \xi_k^\top G^\top P_u G \xi_k\Big) - \tau_1 \Big(1 - \tilde{x}_k^\top Q \tilde{x}_k\Big) - \tau_2 \Big(\delta - \varepsilon_k^\top \varepsilon_k\Big) \geq 0. \tag{42}$$

Similarly, according to the S-procedure, the set $\tilde{x}^\top Q \tilde{x} \leq 1$ is a robustly positively invariant set for the dynamics in (29) if the following inequality holds:

$$\begin{aligned}\Big(1 - \tilde{x}_{k+1}^\top Q \tilde{x}_{k+1}\Big) - \sigma_1 \Big(1 - \tilde{x}_k^\top Q \tilde{x}_k\Big) - \sigma_2 \Big(\delta - \varepsilon_k^\top \varepsilon_k\Big) \\ - \sigma_3 \Big(1 - \xi_k^\top G^\top P_u G \xi_k\Big) - \sigma_4 \Big(\kappa - w_k^\top w_k\Big) \geq 0.\end{aligned} \tag{43}$$

Notice that (38)–(40) imply (42) and (43), which concludes the proof. ■

V. Tube-Based Model Predictive Controller

A. Propagation of States and Error During Detection Operation

Consider the predictions $\hat{x}_k = x_k + \nu_k$ generated by the state predictor in (9), then the resulting control law (considering the MPC action), is described as follows:

$$u_{\bar{k}T+i} = K \hat{x}_{\bar{k}T+i} + c_{\bar{k}T}. \tag{44}$$

In this regard, the predictions $\hat{x}_{\bar{k}T+i}$, for $i \in \mathbb{N}_{\leq T-1}$, are

$$\hat{x}_{\bar{k}T+i} = \Phi_i x_{\bar{k}T} + \Gamma_i c_{\bar{k}T} \tag{45}$$

where $\Phi_0 = I_n$, $\Gamma_0 = 0$, and

$$\Phi_i = (A + BK)^i, \quad \Gamma_i = \sum_{j=0}^{i-1} \big(\Phi_j B\big). \tag{46}$$

Similarly, the plant states $x_{\bar{k}T+i}$ are computed by substituting (44) and (45) in (1), yielding

$$x_{\bar{k}T+i} = \Phi_i x_{\bar{k}T} + \Gamma_i c_{\bar{k}T} + W_i \tag{47}$$

where

$$W_i = A W_{i-1} + E w_{i-1} = \sum_{j=0}^{i-1} A^j E w_{\bar{k}T+j}, \quad W_0 = 0. \tag{48}$$

Consequently, comparing (45) and (47), the prediction error is computed by $\nu_{\bar{k}T+i} = \hat{x}_{\bar{k}T+i} - x_{\bar{k}T+i} = -W_i$. Thus, from $w_k \in \mathcal{W}$, it follows that $\nu_{\bar{k}T+i} \in -\mathcal{W}_i$ with $\mathcal{W}_0 = \emptyset$ and

$$\mathcal{W}_i = A \mathcal{W}_{i-1} \oplus E \mathcal{W}. \tag{49}$$

B. Robust MPC Design

In the proposed approach, a robust MPC action is designed with the slower sample rate, i.e., the control action $c_{\bar{k}T}$ is updated at each T samples. Thus, based on (47), the following model describes the system states at each T samples:

$$x_{(\bar{k}+1)T} = \Phi_T x_{\bar{k}T} + \Gamma_T c_{\bar{k}T} + W_T \tag{50}$$

where according to (46), Φ_T and Γ_T are given by

$$\Phi_T = (A + BK)^T, \quad \Gamma_T = \sum_{j=0}^{T-1} \big(\Phi_j B\big) \tag{51}$$

and $W_T \in \mathcal{W}_T$. Additionally, given the input constraint $\tilde{\mathcal{U}}$, the corresponding input space for (50), with a sample rate of T times the sampling period of (1), is given by $\tilde{\mathcal{U}}_T = T\tilde{\mathcal{U}}$.

Below, the robust control strategy devised in [42] is used for robustly stabilizing (50) to a neighborhood of the origin, while guaranteeing constraint satisfaction and recursive feasibility. This robust MPC scheme first requires the offline computation of the reachable sets for the mismatch between the disturbed system (50) and the nominal system (i.e., nondisturbed). Then, a deterministic MPC with tighter constraints is solved online for the nominal system. At this point, since Φ_T is ensured to be Schur stable by means of the state-feedback $\mathcal{H}_\infty$ controller, there is no need to design a local control law for attenuating the effect of the uncertainty in the prediction. Hence, the error between the disturbed and nominal system is confined within the following reachable set:

$$\bar{\mathcal{X}}(i) = \bigoplus_{j=0}^{i-1} \Big(\Phi_T^j \mathcal{W}_T\Big), \quad \bar{\mathcal{X}}(0) = \emptyset \tag{52}$$

whereas the state-feedback $\mathcal{H}_\infty$ controller plus watermark signal plus RB block is bounded by

$$\bar{\mathcal{U}} = \bigoplus_{j=0}^{T-1} \big(K \Phi_j \mathcal{W}_j \oplus \mathcal{R}\big). \tag{53}$$

Therefore, the following control policy is considered [42]:

$$c_{\bar{k}} = g^*\big(0|\bar{k}T\big) \tag{54}$$

where $g^*(0|\bar{k}T)$ is the optimum point (computed at $\bar{k}T$) of the following H-horizon MPC optimization problem:

$$\min_{g(0),\ldots,g(H-1)} \ \sum_{i=0}^{H-1} \Big(\|x(i)\|_{Q_J}^2 + \|g(i)\|_{R_J}^2\Big) + \Psi(x(H)) \tag{55a}$$
$$\text{s.t.} \quad \bar{x}(i+1) = \Phi_T \bar{x}(i) + \Gamma_T g(i) \tag{55b}$$
$$x(0) = x_{\bar{k}T} \tag{55c}$$
$$\bar{x}(i) \in \mathcal{X} \ominus \bar{\mathcal{X}}(i) \tag{55d}$$
$$g(i) \in \tilde{\mathcal{U}}_T \ominus \bar{\mathcal{U}} \tag{55e}$$
$$\bar{x}(H) \in \Omega \ominus \bar{\mathcal{X}}(H) \tag{55f}$$
$$\forall i \in \mathbb{N}_{\leq H-1}. \tag{55g}$$

The terminal cost $\Psi(\cdot)$ in (55a) is used to ensure the closed-loop stability, and it is computed using a Lyapunov function for a control law that stabilizes the nominal system. Besides, (55f) imposes that the last element of the predicted sequence belongs

to the robust positively invariant (RPI) set Ω. Iterative procedures for computing the maximal RPI set in the state constraint set (and taking into account input constraints) are given in [43]. Additionally, matrices $Q_J = Q_J^\top \succ 0$ and $R_J = R_J^\top \succ 0$ are tuning parameters for the MPC control law.

Remark 5: The parameter T plays an important role in the DRC. On the one hand, from a security point of view, it is desirable to enlarge parameter T due to: 1) during the detection mode, the DRC is resilient to sensor attacks since it is not using unreliable data and 2) the user's detection scheme has more time to detect the attack and certificate the state of the communications network. On the other hand, large values of T affect the system closed-loop performance and may result in an empty solution space for the MPC [empty sets in (55d)–(55f)] or in a reduced domain of attraction. Accordingly, parameter T must be selected to meet the minimum requirements in Assumption 2, while providing an admissible domain of attraction for the upper tier robust MPC controller.

C. DRC Framework

The next result indicates the convergence of the DRC framework, which integrates the prediction-based state-feedback, RB, and MPC, whose are described in the previous sections.

Proposition 1: Provided that the initial state x_0 is a feasible point of (55), and a detector block capable to satisfy Assumptions 1 and 2. Then, the control policy introduced in Section II is capable to robustly steer the system to a neighbourhood of the origin, while guaranteeing robust constraint satisfaction, under any man-in-the-middle attack of the form (6).

Proof: The attack independence follows from the fact that the DRC formulated in Section II operates using only measurements obtained each T samples, which are secure from Assumptions 1 and 2. Regarding the system stability, the $\mathcal{H}_\infty$ controller attenuates the effect of the prediction error ν_k during the detection operation, which from Assumption 1 is bounded on $\nu_k \in \mathcal{W}_{T-1}$. Moreover, the robust MPC controller is formulated for a tightened set of constraints that account for the effect of the watermark signal, the RB, and the attenuated prediction error. Hence, given a feasible x_0, from [42, Th. 8], it follows that $x_k \in \mathcal{X}$, $u_k \in \tilde{\mathcal{U}}$ for all $k \geq 0$ and $x_k \to \bar{\mathcal{X}}(\infty)$ as $k \to \infty$. ■

The design and execution steps for the proposed DRC framework are summarized in Algorithm 1. The control parameters of the prediction-based state-feedback controller and the RB, as well as the MPC ingredients, are designed offline as indicated in the lines 2–5 of the offline phase of Algorithm 1. In particular, a convex optimization problem is solved to compute the gain K [cf. (17)] subject to the constraint (16) while maximizing the scalar ρ. Similarly, the RB parameters A_r, B_r, R_1, and R_2 are obtained based on Theorem 2, in particular (32) and (33), by minimizing $\tilde{\rho}$ under the constraint (31). Finally, the set $\mathcal{R}$ that is used in the MPC problem (55) is computed based on Theorem 3 by maximizing the trace of P_u under the constraints (38) and (40).

Algorithm 1 DRC Framework

OFF-LINE PHASE

1: **Design** the attack detector and the watermark signal such that $\varepsilon_k \in \mathcal{E}$
2: **Compute** the state-feedback gain K using Theorem 1
3: **Compute** the RB gains A_r, B_r, R_1, and R_2 using Theorem 2
4: **Compute** the set $\mathcal{R}$ using Theorem 3
5: **Compute** the MPC ingredients Ω and $\Psi(\cdot)$

ON-LINE PHASE (for each $k \in \mathbb{N}$)

if $k \bmod T = 0$ **then**
  $\hat{u}_k = Kx_k$
  Solve the MPC problem (55) to obtain c_k
else
  $\hat{u}_k = K\hat{x}_k$
end if
$u_k = \hat{u}_k + c_k$
$\bar{u}_k = u_k + \varepsilon_k$
$u_{r,k} = R_1 x_{r,k} + R_2 \bar{u}_k$
$\tilde{u}_k = u_{r,k} + \bar{u}_k$
Check the attack occurrence
if an attack is detected **then**
  Recover the network security
end if
if $k \bmod T = 0$ **then**
  $\hat{x}_{k+1} = Ax_k + Bu_k$
else
  $\hat{x}_{k+1} = A\hat{x}_k + Bu_k$
end if
$x_{r,k+1} = A_r x_{r,k} + B_r \bar{u}_k$

VI. Application Example: Quadruple Tank Process

This section applies the proposed secure-control strategy to a quadruple-tank system subject to attacks to illustrate the defensive capabilities of the DRC strategy and the RB effectiveness for mitigating the watermark signal effect.

The quadruple-tank system [44] is a well-known benchmark used to evaluate control and supervision strategies, and it has been also employed to evaluate secure-control and cyber-attack detection techniques in [11] and [12]. The nonlinear dynamics of the quadruple-tank system are described as follows:

$$\begin{aligned}
\frac{dh_1}{dt} &= -\frac{a_1}{A_1}\sqrt{2gh_1} + \frac{a_3}{A_1}\sqrt{2gh_3} + \frac{\gamma_1 k_1}{A_1}v_1 + e_1 w_1 \\
\frac{dh_2}{dt} &= -\frac{a_2}{A_2}\sqrt{2gh_2} + \frac{a_4}{A_2}\sqrt{2gh_4} + \frac{\gamma_2 k_2}{A_2}v_2 + e_1 w_1 + e_2 w_2 \\
\frac{dh_3}{dt} &= -\frac{a_3}{A_3}\sqrt{2gh_3} + \frac{(1-\gamma_2)k_2}{A_3}v_2 + e_1 w_1 + e_3 w_3 \\
\frac{dh_4}{dt} &= -\frac{a_4}{A_4}\sqrt{2gh_4} + \frac{(1-\gamma_1)k_1}{A_4}v_1 + e_1 w_1 + e_4 w_4 \\
z_1 &= k_c h_1, \quad z_2 = k_c h_2, \quad y_i = h_i \ \forall i = 1, \ldots, 4
\end{aligned} \tag{56}$$

where v_j, for $j \in 1, 2$, is the control input such that $k_j v_j$ is the jth input flow rate, h_i, A_i, and a_i denote, respectively, the liquid level, the cross-section area, and the outlet hole cross-section of the ith tank, g is the gravity acceleration, and $\gamma_j \in [0, 1]$ is the position of the jth valve. The values of these parameters

TABLE I
QUADRUPLE TANK PROCESS PARAMETERS

Parameter	Value	Unit
$A_1 = A_3$	28	cm^2
$A_2 = A_4$	32	cm^2
$a_1 = a_3$	0.071	cm^2
$a_2 = a_4$	0.057	cm^2
k_c	0.5	V/cm
g	981	cm/s^2
(h_1^o, h_2^o)	(12.4, 12.7)	cm
(h_3^o, h_4^o)	(1.8, 1.4)	cm
(v_1^o, v_2^o)	(3, 3)	V
(k_1^o, k_2^o)	(3.33, 3.35)	$cm^3/V\ s$
(γ_1^o, γ_2^o)	(0.7, 0.6)	–
e_1	0.05	–
$e_2 = e_3 = e_4$	0.01	–

are given in Table I, and the superscript ^{o} indicates the chosen operation point that is suggested by [44].

Linearizing (56) around the operating point and using Euler discretization with a sampling time of 1 s, a linear discrete-time model as (1) is obtained, describing the dynamics of $\Delta h_{k,i} = h_{k,i} - h_{k,i}^o$ and $\Delta v_{k,i} = v_{k,i} - v_{k,i}^o$ with

$$x_k^\top = \begin{bmatrix}\Delta h_{k,1}^\top\ \Delta h_{k,2}^\top\ \Delta h_{k,3}^\top\ \Delta h_{k,4}^\top\end{bmatrix},\ u_k^\top = \begin{bmatrix}\Delta v_{k,1}^\top\ \Delta v_{k,2}^\top\end{bmatrix}$$
$$z_k^\top = \begin{bmatrix}\Delta z_{k,1}^\top\ \Delta z_{k,2}^\top\end{bmatrix},\ C = \begin{bmatrix}k_c I_2\ 0_{2\times 2}\end{bmatrix},\quad D = 0_{2\times 2}$$
$$A = \begin{bmatrix} -\frac{1}{T_1} & 0 & \frac{A_3}{A_1 T_3} & 0 \\ 0 & -\frac{1}{T_2} & 0 & \frac{A_3}{A_1 T_3} \\ 0 & 0 & -\frac{1}{T_3} & 0 \\ 0 & 0 & 0 & -\frac{1}{T_4} \end{bmatrix},\ B = \begin{bmatrix} \frac{\gamma_1^o k_1^o}{A_1} & 0 \\ 0 & \frac{\gamma_2^o k_2^o}{A_2} \\ 0 & \frac{(1-\gamma_2^o)k_2^o}{A_3} \\ \frac{(1-\gamma_1^o)k_1^o}{A_4} & 0 \end{bmatrix}$$
$$E = \begin{bmatrix} e_1 & 0 & 0 & 0 \\ e_1 & e_2 & 0 & 0 \\ e_1 & 0 & e_3 & 0 \\ e_1 & 0 & 0 & e_4 \end{bmatrix},\ T_i = \frac{A_i}{a_i}\sqrt{\frac{2h_i^o}{g}}.$$

The system states and inputs satisfy the elementwise constraints $h_i \in [0, 20]$ cm, $u_1, u_2 \in [-3, 3]$. Besides, the disturbance vector $w_k^\top = [w_1^\top\ w_2^\top\ w_3^\top\ w_4^\top]$ is assumed to be a uniformly distributed random variable within the disturbance set $\mathcal{W} = \{w \in \mathbb{R}^4 | w^\top w \le \sqrt{2}\}$.

In this example, it is considered that a malicious attacker launches a replay attack on the system outputs. Notably, the attacker secretly records the output signal y_k in the time interval $k \in [2, 19]$. Hence, following the attack description (6), the received output signal is:

$$\tilde{y}_k = \begin{cases} y_{2+T_a}, & \text{if } k \ge k_{\text{rep}} \\ y_k, & \text{otherwise} \end{cases} \tag{57}$$

where $T_a = k\%18$, and the data replay starts at $k = k_{\text{rep}}$.

A. Attack Detector

In the sequel, the system operation is assessed by means of an anomaly detector fed with the input signal $\bar{u}_k$ and the (possible compromised) output signal $\tilde{y}_k$ (cf. Fig. 2). In particular, the system is evaluated according to the values adopted by a residual signal that compares the received system outputs with its estimates generated using a Luenberger observer. The attack detector is described as follows:

$$\begin{cases} \hat{x}_{o,k+1} = (A - L)\hat{x}_{o,k} + B\bar{u}_k + L\tilde{y}_k \\ r_k = \tilde{y}_k - \hat{x}_{o,k} \end{cases} \tag{58}$$

where $r_k \in \mathbb{R}^n$ is the residual, $\hat{x}_{o,k} \in \mathbb{R}^n$ is the state of the Luenberger observer, and the gain L is designed to ensure that $A - L$ is Schur. Additionally, by taking into account the bounds on process disturbances w_k, a healthy steady-state residual set denoted as $\mathcal{R}_H$ is computed, in such a way that an alarm is triggered whenever $r_k \notin \mathcal{R}_H$.

Watermark Signal: A watermarking strategy is used for evaluating the DRC. In particular, a set of finite N-step sequences to guarantee the attack detection until the Nth sample. As proposed in [45], the open-loop input sequences are designed by solving a mixed-integer quadratic program to guarantee the separability of the reachable zonotopic set of residuals considering the uncertainties bounded by (2).[1] The sequences are specifically devised to detect replay attacks and exploit the temporal mismatch between the record and replay phases in order to ensure that if under attack, the residual signal must satisfy $r_{k'+N} \notin \mathcal{R}_H$. Additionally, the sequences are designed to be within a preestablished set $\mathcal{E}$. Notice that it is highly unlikely that the attacker's signal is similar to the watermark since the watermarking signal is inherently random, i.e., a random sequence of the set of designed signals is used every time. For more details on the watermarking design methodology, the reader may refer to [45].

Remark 6: In this simulation example, the replay attack in (57) and the residual-based attack detector with watermarking described in Section VI-A are considered to evaluate the proposed DRC framework. However, any effective watermarking-based attack detector can be used under Assumptions 1 and 2 for $\varepsilon \in \mathcal{E}$ [cf. (10)], and the security is guaranteed for generic deception attacks as described in (6).

B. Dual-Rate Controller and RB Design

The application of the Theorems 1 and 2 to design, respectively, the state-feedback controller and the RB, provides the following values of K, A_r, B_r R_1, and R_2[2]:

$$K = \begin{bmatrix} -4.5070 & 0.0305 & -0.1977 & -0.0003 \\ -0.0091 & -14.5692 & -0.0225 & -0.5421 \end{bmatrix}$$
$$A_r = \begin{bmatrix} -0.2194 & -0.1905 & -0.0226 & -0.0193 \\ -0.2955 & -0.1934 & -0.0170 & -0.0138 \\ -0.3048 & -0.5440 & 0.4596 & -0.0290 \\ -0.3154 & -0.2200 & -0.0193 & 0.4704 \end{bmatrix}$$
$$B_r = \begin{bmatrix} -0.0230 & -0.0180 \\ -0.0251 & -0.0198 \\ -0.0284 & -0.0181 \\ -0.0256 & -0.0206 \end{bmatrix},\ R_2 = \begin{bmatrix} -1.0360 & -0.0322 \\ -0.0509 & -1.0286 \end{bmatrix}$$
$$R_1 = \begin{bmatrix} -5.3725 & -0.5566 & 0.3579 & 1.4597 \\ -1.2907 & -15.7439 & -1.1248 & 7.7786 \end{bmatrix}.$$

[1]The YALMIP parser and the GUROBI solver are used to compute the watermarking signals.

[2]The YALMIP parser and the MOSEK solver are used to compute the control parameters.

TABLE II
COMPARISON BETWEEN THE RMS QUADRUPLE-TANK RESPONSES

Control structure	States (RMS)			
	$\Delta h_{k,1}$	$\Delta h_{k,2}$	$\Delta h_{k,3}$	$\Delta h_{k,4}$
DRC without watermarking	0.0963	0.0955	0.0871	0.0986
DRC with watermarking	0.2294	0.2194	0.1368	0.0968
DRC with watermarking and RB	0.1161	0.1450	0.0939	0.0986
State-feedback with watermarking	2.6073	3.2341	1.4061	0.1328

An MPC with horizon $H = 5$ is designed for $T = 20$ and matrices $Q_J = I_4$ and $R_J = 0.5I_2$. Theorem 3 is used to compute the set $\mathcal{R}$ with

$$P_u = \begin{bmatrix} 0.0025 & -0.0003 \\ -0.0003 & 0.0001 \end{bmatrix}.$$

C. Results

To show the advantages of using the proposed DRC scheme for defending the system from cyber attacks, the DRC is compared to the usual $\mathcal{H}_\infty$ state-feedback control where the same K designed above is employed without predictor, i.e., the state-feedback controller receives all the measurements. Furthermore, the responses of the DRC strategy with and without RB are also compared to evaluate the effect of the RB in the system and in the attack detection.

In particular, the simulation considers the occurrence of sensors' replay attack at $k_{\text{rep}} = 85$, within the detection phase starting at $k = 80$. Under Assumption 1, the attack is mitigated at the next multiple of T after the attack detection, i.e., a secure measurement is obtained at $k = 100$. However, the attack is repeated in the next cycles to highlight the effect of the DRC.

The simulations results are depicted in Figs. 3 and 4. The system state trajectories are depicted in Fig. 3, and the replay attack signal $\tilde{y}_k$, defined in (57), are shown in Fig. 5. Notice that the DRC is able to prevent the replay attack effects with and without RB [Fig. 3(a)–(c)], while the state-feedback control is more sensitive to the attack occurrence as depicted in Fig. 3(d). By comparing Fig. 3(a) and (c), it is clear the RB effectively reduces the impact of the watermarking in the system trajectories. Table II compares the root mean square (RMS) of the responses depicted in Fig. 3. It indicates the advantages of the DRC when compared with state-feedback controller. In particular, while the watermarking deteriorates the performance, the response of DRC with RB is very similar to the response without watermarking.

Fig. 4 depicts the attack detection results. In Fig. 4(a), the detector is not able to detect anything (residuals within the healthy residual set $\mathcal{R}_H$ in blue), because there is no watermark injection, and thus, the replay attack cannot be revealed without an active detection method. The watermark signal injection is enough to ensure the detection with DRC or state-feedback control as depicted in Fig. 4(b) and (d). Moreover, Fig. 4(c) indicates that the RB is not affecting the detection ability, although it is able to reduce the watermarking effect in the system trajectories. That is possible due to the choice of the input signals to the detector that excludes RB signal.

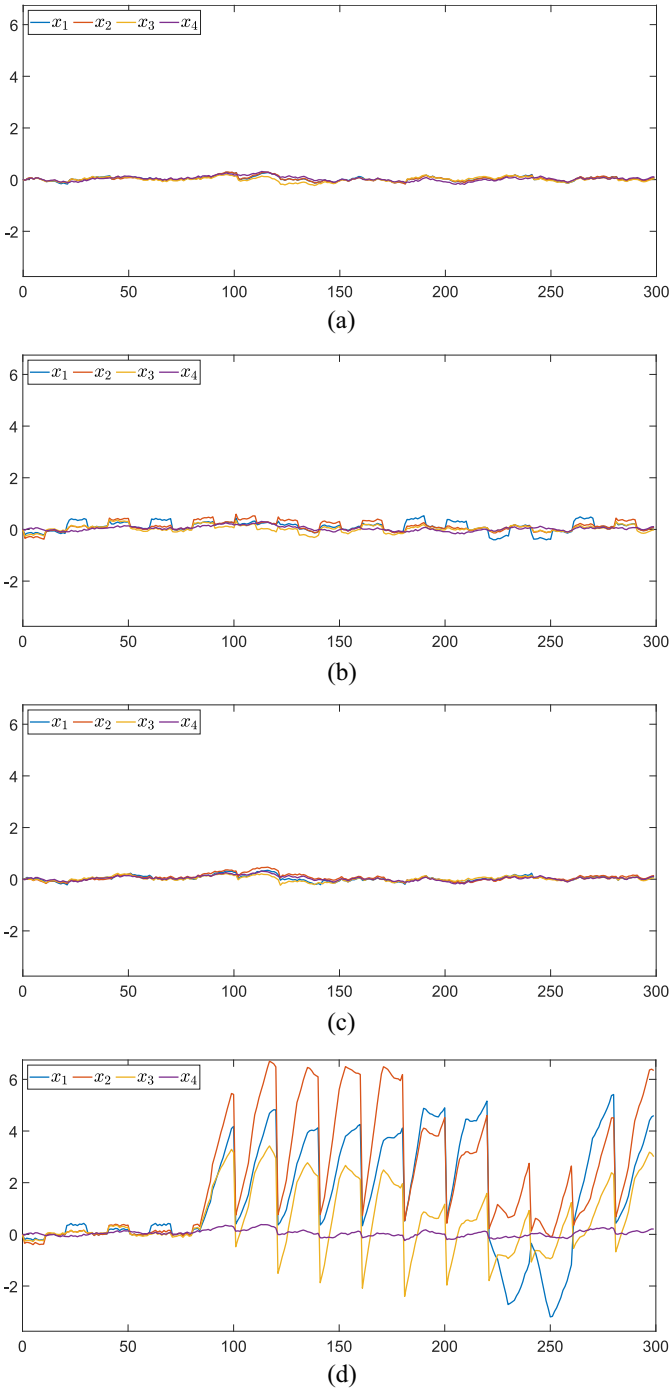

Fig. 3. States' responses under replay attack occurring at $k = 85$. (a) Quadruple-tank responses for DRC without watermarking. (b) Quadruple-tank responses for DRC with watermarking and without RB. (c) Quadruple-tank responses for DRC with watermarking and RB. (d) Quadruple-tank responses for state-feedback control with watermarking.

VII. CONCLUSION

This article has presented a novel secure-control based on DRC framework. This control scheme ensures the stability of the system using an MPC and a predictor-based $\mathcal{H}_\infty$ controller that replaces the untrustworthy measurements by predictions until the measurements are considered secure. Since the security certification is usually done by an attack detector after injecting watermarking signals, it is proposed

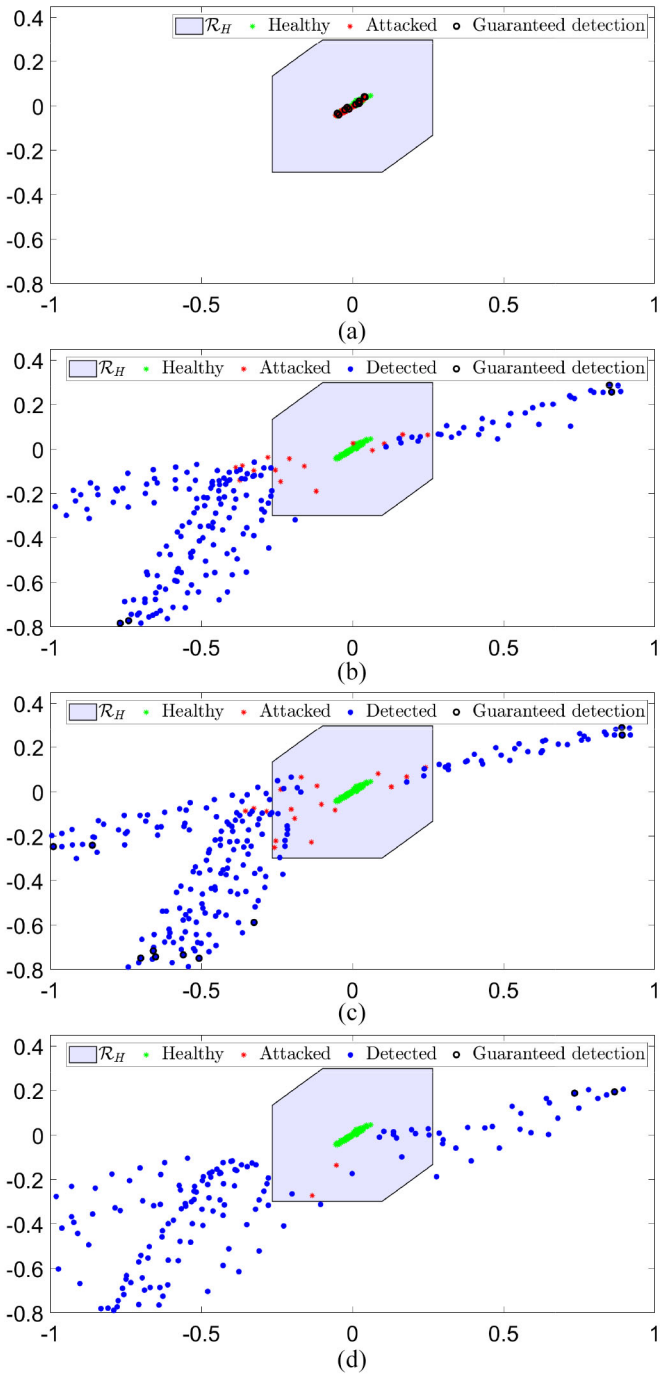

Fig. 4. Attack detection results where it is verified whether the residuals belong or not to the healthy set $\mathcal{R}_H$ (blue set). (a) Attack detection without watermarking. (b) Attack detection with DRC without RB. (c) Attack detection with DRC and RB. (d) Attack detection with state-feedback control.

to use an RB to attenuate the performance degradation due to watermarking. The proposed secure-control framework disregards any assumption on the attacker behavior, since only predictions are used while the measurements are not reliable. The simulation results show the effectiveness of the DRC in both: healthy and under attack operation. In addition, the results also illustrate the capability of the RB to alleviate the harmful effect of injecting a watermark signal during the controller's open-loop operation, while preserving the detection capabilities of the watermarking strategy.

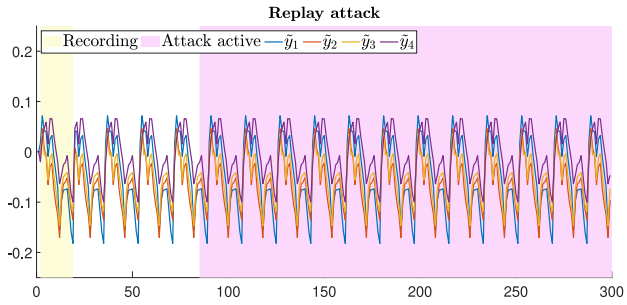

Fig. 5. Replay attack description. The samples within the interval [2, 19] are recorded (time interval with yellow background), and they are replayed from the instant $k_{\text{rep}} = 85$ (time interval with magenta background).

Finally, three promising research directions have been identified, namely: the joint design of the watermarking strategy and the DRC to improve closed-loop operation; the application of the DRC to the networked control context where redundant information present in sensor networks could be used to close the loop when there is no local reliable measurement as proposed in [23], and the extension of double-tier schemes to aperiodic implementations with the intention of enlarging the length of the detection operation.

REFERENCES

[1] D. Rotondo, H. S. Sánchez, V. Puig, T. Escobet, and J. Quevedo, "A virtual actuator approach for the secure control of networked LPV systems under pulse-width modulated DoS attacks," *Neurocomputing*, vol. 365, no. 4, pp. 21–30, 2019.

[2] P. S. Pessim, M. L. Peixoto, R. M. Palhares, and M. J. Lacerda, "Static output-feedback control for cyber-physical LPV systems under DoS attacks," *Inf. Sci.*, vol. 563, pp. 241–255, Jul. 2021.

[3] X. Ge, Q.-L. Han, M. Zhong, and X.-M. Zhang, "Distributed Krein space-based attack detection over sensor networks under deception attacks," *Automatica*, vol. 109, Nov. 2019, Art. no. 108557.

[4] S. Weng, D. Yue, and C. Dou, "Secure distributed optimal frequency regulation of power grid with time-varying voltages under cyberattack," *Int. J. Robust Nonlinear Control*, vol. 30, no. 3, pp. 894–909, 2020.

[5] J. Tian, B. Wang, T. Li, F. Shang, and K. Cao, "Coordinated cyber-physical attacks considering DoS attacks in power systems," *Int. J. Robust Nonlinear Control*, vol. 30, no. 11, pp. 4345–4358, 2020.

[6] S. Nateghi, Y. Shtessel, and C. Edwards, "Cyber-attacks and faults reconstruction using finite time convergent observation algorithms: Electric power network application," *J. Frankl. Inst.*, vol. 357, no. 1, pp. 179–205, 2020.

[7] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Resilient operation of heterogeneous sources in cooperative DC microgrids," *IEEE Trans. Power Electron.*, vol. 35, no. 12, pp. 12601–12605, Dec. 2020.

[8] N. Kadosh, A. Frid, and M. Housh, "Detecting cyber-physical attacks in water distribution systems: One-class classifier approach," *J. Water Resour. Plan. Manag.*, vol. 146, no. 8, 2020, Art. no. 4020060.

[9] Y. Tang, D. Zhang, D. W. Ho, W. Yang, and B. Wang, "Event-based tracking control of mobile robot with denial-of-service attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 9, pp. 3300–3310, Sep. 2020.

[10] M. Ghanavati, A. Chakravarthy, and P. P. Menon, "Analysis of automotive cyber-attacks on highways using Partial differential equation models," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 4, pp. 1775–1786, Dec. 2018.

[11] H. S. Sánchez, D. Rotondo, T. Escobet, V. Puig, and J. Quevedo, "Bibliographical review on cyber attacks from a control oriented perspective," *Annu. Rev. Control*, vol. 48, pp. 103–128, 2019.

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

[13] C. Peng, H. Sun, M. Yang, and Y.-L. Wang, "A Survey on Security Communication and Control for Smart Grids under Malicious Cyber Attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 8, pp. 1554–1569, Aug. 2019.

[14] Z. Guo, L. Shi, D. E. Quevedo, and D. Shi, "Secure state estimation against integrity attacks: A Gaussian mixture model approach," *IEEE Trans. Signal Process.*, vol. 67, no. 1, pp. 194–207, Jan. 2019.

[15] W. Ao, Y. D. Song, and C. Y. Wen, "Distributed secure state estimation and control for CPSs under sensor attacks–A finite time approach," *Zidonghua Xuebao/Acta Automatica Sinica*, vol. 45, no. 1, pp. 174–184, 2019.

[16] J. Huang, D. W. Ho, F. Li, W. Yang, and Y. Tang, "Secure remote state estimation against linear man-in-the-middle attacks using watermarking," *Automatica*, vol. 121, no. 4, 2020, Art. no. 109182.

[17] A. Sargolzaei, K. Yazdani, A. Abbaspour, C. D. Crane, and W. E. Dixon, "Detection and mitigation of false data injection attacks in networked control systems," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4281–4292, Jun. 2020.

[18] T. A. Severson, B. Croteau, E. J. Rodríguez-Seda, K. Kiriakidis, R. Robucci, and C. Patel, "A resilient framework for sensor-based attacks on cyber–Physical systems using trust-based consensus and self-triggered control," *Control Eng. Pract.*, vol. 101, Aug. 2020, Art. no. 104509.

[19] X. Meng, N. Zhou, and Q. Wang, "Improved distributed event-triggered control for inverter-based AC microgrids under deceptive cyberattacks," *Int. J. Elect. Power Energy Syst.*, vol. 120, Sep. 2020, Art. no. 106000.

[20] W. He, X. Gao, W. Zhong, and F. Qian, "Secure impulsive synchronization control of multi-agent systems under deception attacks," *Inf. Sci.*, vol. 459, pp. 354–368, Aug. 2018.

[21] S. Han, S. K. Kommuri, and S. Lee, "Affine transformed IT2 fuzzy event-triggered control under deception attacks," *IEEE Trans. Fuzzy Syst.*, vol. 29, no. 2, pp. 322–335, Feb. 2021.

[22] X. Sun, Z. Gu, F. Yang, and S. Yan, "Memory-event-trigger-based secure control of cloud-aided active suspension systems against deception attacks," *Inf. Sci.*, vol. 543, pp. 1–17, Jan. 2021.

[23] S. Chen, Z. Wu, and P. D. Christofides, "A cyber-secure control-detector architecture for nonlinear processes," *AIChE J.*, vol. 66, no. 5, pp. 1–18, 2020.

[24] X. Xie, D. Yue, and C. Peng, "Relaxed real-time scheduling stabilization of discrete-time Takagi–Sugeno fuzzy systems via an alterable-weights-based ranking switching mechanism," *IEEE Trans. Fuzzy Syst.*, vol. 26, no. 6, pp. 3808–3819, Dec. 2018.

[25] S. Chen, Z. Wu, and P. D. Christofides, "Cyber-attack detection and resilient operation of nonlinear processes under economic model predictive control," *Comput. Chem. Eng.*, vol. 136, May 2020, Art. no. 106806.

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

[27] C. Fang, Y. Qi, P. Cheng, and W. X. Zheng, "Optimal periodic watermarking schedule for replay attack detection in cyber-Physical systems," *Automatica*, vol. 112, Feb. 2020, Art. no. 108698.

[28] M. Porter, P. Hespanhol, A. Aswani, M. Johnson-Roberson, and R. Vasudevan, "Detecting generalized replay attacks via time-varying dynamic watermarking," *IEEE Trans. Autom. Control*, vol. 66, no. 8, pp. 3502–3517, Aug. 2021.

[29] A. Abdelwahab, W. Lucia, and A. Youssef, "Set-theoretic control for active detection of replay attacks with applications to smart grid," in *Proc. Conf. Control Technol. Appl. (CCTA)*, 2020, pp. 1004–1009.

[30] Á. Cuenca, D. J. Antunes, A. Castillo, P. García, B. A. Khashooei, and W. P. Heemels, "Periodic event-triggered sampling and dual-rate control for a wireless networked control system with applications to UAVs," *IEEE Trans. Ind. Electron.*, vol. 66, no. 4, pp. 3157–3166, Apr. 2019.

[31] J. Alcaina, A. Cuenca, J. Salt, V. Casanova, and R. Pizá, "Delay-independent dual-rate PID controller for a packet-based networked control system," *Inf. Sci.*, vol. 484, no. 5, pp. 27–43, 2019.

[32] M. Farina, X. Zhang, and R. Scattolini, "A hierarchical multi-rate MPC scheme for interconnected systems," *Automatica*, vol. 90, pp. 38–46, Apr. 2018.

[33] M. Naghnaeian, N. H. Hirzallah, and P. G. Voulgaris, "Security via multirate control in cyber-physical systems," *Syst. Control Lett.*, vol. 124, pp. 12–18, Feb. 2019.

[34] I. Bessa, V. Puig, and R. M. Palhares, "TS fuzzy reconfiguration blocks for fault tolerant control of nonlinear systems," *J. Frankl. Inst.*, vol. 357, no. 8, pp. 4592–4623, 2020.

[35] J. H. Richter, *Reconfigurable Control of Nonlinear Dynamical Systems: A Fault-Hiding Approach*. Berlin, Germany: Springer, 2011.

[36] I. Bessa, V. Puig, and R. M. Palhares, "Passivation blocks for fault tolerant control of nonlinear systems," *Automatica*, vol. 125, Mar. 2021, Art. no. 109450.

[37] Y. Wang, D. Rotondo, V. Puig, and G. Cembrano, "Fault-tolerant control based on virtual actuator and sensor for discrete-time descriptor systems," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 67, no. 12, pp. 5316–5325, Dec. 2020.

[38] C. Trapiello and V. Puig, "Set-based replay attack detection in closed-loop systems using a plug & play watermarking approach," in *Proc. 4th Conf. Control Fault Toler. Syst.*, Sep. 2019, pp. 330–335.

[39] R. M. G. Ferrari and A. M. H. Teixeira, "A switching multiplicative watermarking scheme for detection of stealthy cyber-attacks," *IEEE Trans. Autom. Control*, vol. 66, no. 6, pp. 2558–2573, Jun. 2021.

[40] R. M. G. Ferrari and A. M. H. Teixeira, "Detection and isolation of routing attacks through sensor watermarking," in *Proc. Amer. Control Conf.*, 2017, pp. 5436–5442.

[41] G. Franze, W. Lucia, and F. Tedesco, "Resilient model predictive control for constrained cyber-physical systems subject to severe attacks on the communication channels," *IEEE Trans. Autom. Control*, early access, May 27, 2021, doi: 10.1109/TAC.2021.3084237.

[42] L. Chisci, J. A. Rossiter, and G. Zappa, "Systems with persistent disturbances: Predictive control with restricted constraints," *Automatica*, vol. 37, no. 7, pp. 1019–1028, 2001.

[43] I. Kolmanovsky and E. G. Gilbert, "Theory and computation of disturbance invariant sets for discrete-time linear systems," *Math. Problem Eng.*, vol. 4, no. 4, pp. 317–367, 1998.

[44] K. H. Johansson, "The quadruple-tank process: A multivariable laboratory process with an adjustable zero," *IEEE Trans. Control Syst. Technol.*, vol. 8, no. 3, pp. 456–465, May 2000.

[45] C. Trapiello and V. Puig, "Input design for active detection of integrity attacks using set-based approach," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 11094–11099, 2020.

Iury Bessa received the B.Sc. and master's degrees in electrical engineering from the Federal University of Amazonas, Manaus, Brazil, in 2014 and 2015, respectively. He is currently pursuing the Ph.D. degree in electrical engineering with the D!FCOM Laboratory, Federal University of Minas Gerais, Belo Horizonte, Brazil.

During his Ph.D., he was a Visiting Scholar with the University of Catalonia, Barcelona, Spain, from February 2020 to December 2020. Since 2015, he has been an Assistant Professor with the Department of Electricity and is a part of the e-Controls Research Group, Federal University of Amazonas. His research interests include control theory, fault-tolerant control, fault detection, diagnosis and prognosis, formal verification and synthesis, learning-based control, cyber-physical systems, and computational intelligence.

Carlos Trapiello received the B.Sc. degree in aerospace engineering from the Universidad Politécnica de Madrid, Madrid, Spain, in 2015, and the M.Sc. degree in automatic control & robotics and the Ph.D. degree in control engineering from the Universitat Politécnica de Catalunya-BarcelonaTech, Barcelona, Spain, in 2018 and 2021, respectively.

He is currently on a postdoctoral stay with the UMR 5218, IMS Laboratory, Bordeaux, France.

Vicenç Puig received the B.Sc. and M.Sc. degrees in telecommunications engineering and the Ph.D. degree in automatic control, vision, and robotics from the Universitat Politécnica de Catalunya-BarcelonaTech (UPC), Barcelona, Spain, in 1993 and 1999, respectively.

He is currently a Full Professor with the Automatic Control Department, UPC, and a Researcher with the Institut de Robòtica i Informàtica Industrial, CSIC-UPC. He is also the Director of the Automatic Control Department and the Head of the Research Group on Advanced Control Systems, UPC. He has developed important scientific contributions in the areas of fault diagnosis and fault-tolerant control, using interval, and linear-parameter-varying models using set-based approaches. He has participated in more than 20 European and national research projects in the last decade. He has also led many private contracts with several companies and has published more than 220 journal articles as well as over 500 contributions in international conference/workshop proceedings. He has supervised over 25 Ph.D. dissertations and over 50 master theses/final projects.

Prof. Puig was the General Chair of the Third IEEE Conference on Control and Fault-Tolerant Systems (SysTol 2016) and the IPC Chair of IFAC Safeprocess 2018. He is also the Chair of the IFAC Safeprocess TC Committee 6.4.

Reinaldo Martínez Palhares (Member, IEEE) received the Ph.D. degree in electrical engineering from the UNICAMP, Campinas, Brazil, in 1998.

He is currently a Full Professor with the Department of Electronics Engineering, Federal University of Minas Gerais, Belo Horizonte, Brazil. His main research interests include robust control, fault detection, diagnosis and prognosis, and artificial intelligence.

Prof. Palhares has been serving as an Associate Editor for the IEEE TRANSACTIONS ON FUZZY SYSTEMS, IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, and *Sensors*. He had also served as a Guest Editor for the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS—Special Section on "Artificial Intelligence in Industrial Systems," the IEEE/ASME TRANSACTIONS ON MECHATRONICS Focused Section on "Real-time Monitoring, Diagnosis, and Prognosis and Health Management for Electric Vehicles" and the Focused Section on "Health Monitoring, Management and Control of Complex Mechatronic System," and also the *Journal of The Franklin Institute*—Special Section on "Recent Advances on Control and Diagnosis via Process Measurements." He is a member of the Conference Board of the IFAC for the term 2020–2023, and currently a member of the IFAC TC 3.2 "Computational Intelligence in Control"; IFAC TC 6.4 "SAFEPROCESS"; IEEE-IES TC on Data-Driven Control and Monitoring (TC-DDCM); and IEEE TC on Robust and Complex Systems. For more information, see http://www.ppgee.ufmg.br/∼palhares.