Replay attack detection using a zonotopic KF and LQ approach

Carlos Trapiello[1,2] and Vicenç Puig[1,2]

Abstract— **This paper exploits the analogy between the stochastic and zonotopic Kalman filters with the aim of formulating a metric that allows to assess the impact of an external zonotopically bounded signal in an state estimate optimal control scheme. To that end, the concept of linear quadratic zonotopic (LQZ) controller is introduced. Besides, the design of a zonotopically bounded watermarking signal such that enforces replay attack detectability is also addressed. The proposed detection scheme takes advantage of the observability loss of an *a priori* known exogenous signal during the replay phase of the attack. Consequently, by injecting the corresponding estimation error generated by a set-based observer, a zonotopically bounded signal such that imposes replay attack detectability is achieved. A numerical example is provided.**

I. Introduction

During the last decade, issues related to cyber security have experienced a great increase in the interest they arouse in the automatic control community [1]. In this regard, a growing number of publications have focused on different aspects related to cyber security in control systems, such as: the analysis of vulnerabilities of cyber-physical systems (CPS) to external attacks [2], the modelling of the different attack policies to which a networked control system is exposed [3] or the development of security indices in order to assess the protection of the system [4].

In this paper, we will focus attention on the design of strategies to detect deception attacks, that is, those attacks that are able to remain undetected by deceiving the monitoring algorithms that supervise the system operation. A particular kind of deception attacks are the so-called replay attacks, a two-phase attack where the attacker first records data from the sensors and then replays the data back with the intention of masking the injection of an external signal that distorts the system operation. Consequently, replay attacks appear as a very plausible scenario since the attacker does not need to have a detailed knowledge of the system model.

Some of the central works regarding the detectability of replay attacks from an automatic control perspective have focused on analysing the attack in stationary Gaussian processes. Accordingly, in the pioneering work [5], an external Gaussian signal is injected in order to increase the attack detection rate of a statistical detector. That work was further extended in [6], where the term *physical watermarking* was first introduced to refer to the strategies designed to authenticate the correct operation of CPSs. Other works like [7], enforce the replay attack detectability in Gaussian processes by including an additive watermark signal generated by a dynamical system. Besides, in [8], the authors propose a stochastic game approach to derive an optimal control policy to switch between optimal (nonsecure) and secure (suboptimal) controllers.

All the previous works have in common that they are built upon assumptions on the Gaussian probability distribution of the uncertainty variables. However, conversely to the stochastic paradigm, set-membership techniques rely on characterizing the uncertainty variables to be unknown but bounded within some sets. The set-membership approach has evolved in parallel to stochastic techniques, and has proven to yield good results in control-related problems such as state estimation, fault diagnosis, etc.

Among the different set representations used in the literature, we will focus on zonotopes [9], which consist on a special type of symmetric polytopes whose shape is implicitly represented by a rectangular matrix. A work of special interest is [10], where, by introducing the notion of the covariation of a zonotope, the author proposes a robust state observer for which, by minimizing the weighted Frobenius norm (F_W-radius) of the bounding zonotope, expressions analogous to the stochastic Kalman filter are obtained. This analogy between zonotope-based set-membership approaches and stochastic approaches will be exploited in the present work with the aim of proposing a set-based counterpoint to the replay attack detection schemes already existing in the literature.

According to the aforementioned, the contribution of this paper is twofold: 1) an optimal controller for a discrete linear time-invariant system operating based on the estimates performed by a zonotopic Kalman Filter (ZKF) is formulated. This gives rise to the so-called linear quadratic zonotopic (LQZ) controller, the zonotope-based analogous of linear quadratic Gaussian (LQG) controllers. By proceeding in this manner, we are able to formulate a metric to quantify the performance loss in the infinity horizon control problem, and thus, assess the impact that a zonotopically bounded watermarking signal will have on the system; 2) the design of a zonotopically bounded signal for detecting replay attacks. The design of such signal bases its operation on the fact that the observability of an exogenous signal known by the defender is lost during the replay phase. Note that, since using set-based approaches the detectability of the attack can be guaranteed, the performance degradation/detectability rate trade-off existing in stochastic approaches is modified

This work has been partially funded by AGAUR ACCIO RIS3CAT UTILITIES 4.0 – P7 SECUTIL and by SMART Project (ref. num. EFA153/16 Interreg Cooperation Program POCTEFA 2014-2020).

[1] Research Center for Supervision, Safety and Automatic Control (CS2AC), Universitat Politècnica de Catalunya (UPC), Spain carlos.trapiello@upc.edu.

[2] Institut de Robòtica i Informàtica Industrial, CSIC-UPC, Llorens i Artigas 4-6, 08028 Barcelona, Spain.

by the performance degradation/detection speed trade-off.

The remainder of the paper is organized as follows: Section II introduces some preliminary concepts. The LQZ controller is presented in Section III. Section IV is devoted to the characterization of the replay attack, while Section V presents the proposed attack detection scheme. In Section VI, a numerical example is presented in order to exemplify the validity of the proposal. Finally, the main conclusions are drawn in Section VII.

II. Preliminaries

This work makes use of zonotopic sets in generator representation: $Z = \langle c, H\rangle \subset \mathbb{R}^n$, where $c \in \mathbb{R}^n$ denotes the center and $H \in \mathbb{R}^{n\times m}$ the generator matrix of a zonotope of order m/n [9]. Besides, given $\langle c, H\rangle$ the following size criterion will be used (see [10] for detailed explanation including the weighted Frobenius radius)

Definition 1 (F-Radius): The F-radius of $\langle c, H\rangle$ is the Frobenius norm of H : $\|\langle c,H\rangle\|_F = \|H\|_F = \sqrt{tr[H^TH]}$.

Definition 2 (Covariation): The covariation of the zonotope $\langle c, H\rangle$ is $cov(\langle c,H\rangle) = HH^T$.

Accordingly, minimizing the F-radius of a zonotope $\langle c, H\rangle$ is equivalent to minimizing the trace of its covariation matrix $P = HH^T$, i.e. $tr[P] = \|H\|_F^2$.

Previous definition of the covariation of a zonotope is the fundamental point on which it is based the zonotopic Kalman filter (ZKF) derived in [10], such that it becomes the bounded-error counterpart of the standard stochastic Kalman filter. Consequently, in order to quantify the performance loss of a given variable $x \in \langle c, H\rangle$, let us define the deterministic counterpart of the expected value as

Definition 3 (Quadratic term quantification): Given a square matrix $S \in \mathbb{R}^{n\times n}$ and the unknown but zonotopically bounded vector $x \in \langle c, H\rangle \subset \mathbb{R}^n$. The value of the quadratic term x^TSx is quantified through the following operator

$$\mathscr{Q}[x^TSx] = c^TSc + Tr[SP] \tag{1}$$

with $P = cov(\langle c,H\rangle) = HH^T$.

Note that, previous definition matches the expected value for $x \sim \mathscr{N}(c,P)$, a Gaussian random vector centred at c with covariance P. This analogy between the covariation of a zonotope and the covariance will be used as a bridge between the error-bounded and the stochastic fields.

III. LQZ control

This section introduces the design of an optimal controller based on the estimates of a ZKF, as well as the cost obtained in the associated quadratic loss function. The systems under consideration are discrete linear time-invariant (LTI) systems subject to unknown but bounded uncertainties of the form

$$x_{k+1} = Ax_k + Bu_k + Ew_k \tag{2a}$$
$$y_k = Cx_k + Fv_k \tag{2b}$$

where $x_k \in \mathbb{R}^{n_x}$ is the state vector, $u_k \in \mathbb{R}^{n_u}$ an exogenous input signal and $y_k \in \mathbb{R}^{n_y}$ the output vector. The initial state is assumed to belong to the zonotope $x_0 \in \langle c_0, H_0\rangle$. Besides, process disturbances $w_k \in \mathbb{R}^{n_w}$ and sensors noise $v_k \in \mathbb{R}^{n_v}$ are assumed to be confined within the zonotopic sets

$$w_k \in \langle 0, I_{n_w}\rangle \qquad v_k \in \langle 0, I_{n_v}\rangle \qquad \forall k \geq 0 \tag{3}$$

where I_{n_w} and I_{n_v} are identity matrices of size $n_w \times n_w$ and $n_v \times n_v$, respectively.

Assumption 1: The pair (A,B) is assumed to be controllable and the pair (A,C) is assumed to be observable.

A. Zonotopic KF

According to [10], given an initial state such that $x_0 \in \langle c_0, H_0\rangle$, then, by recursively defining the center estimate c_k and the generator matrix H_k such that

$$c_{k+1} = (A - G_kC)c_k + Bu_k + Gy_k \tag{4a}$$
$$H_{k+1} = [(A - G_kC)H_k,\ E,\ -G_kF] \tag{4b}$$

the state inclusion property $x_k \in \langle c_k, H_k\rangle$ holds $\forall k \geq 0$.

Furthermore, the optimal observer gain G^* minimizing the F-radius of the prediction zonotope $\langle c_{k+1}, H_{k+1}\rangle$ is given by

$$G_k^* = AK_k^* = AP_kC^T(CP_kC^T + Q_v)^{-1} \tag{5}$$

where $P_k, Q_w \in \mathbb{R}^{n_x\times n_x}$ and $Q_v \in \mathbb{R}^{n_y\times n_y}$ are the covariation matrices

$$P_k = H_kH_k^T \qquad Q_w = EE^T \qquad Q_v = FF^T \tag{6}$$

with matrix P_k satisfying the recursion

$$P_{k+1} = AP_kA^T + Q_w - AP_kC^T(CP_kC^T + Q_v)^{-1}CP_kA^T \tag{7}$$

and matrix $A - G^*C$ Schur stable by Assumption 1.

Remark 1: In order to achieve a practical implementation, the order of the bounding zonotope should be limited. An efficient way to achieve this is through the reduction order operator ($\downarrow_{q,W}$) presented in [10], [11], such that $\langle \bar{H}\rangle = \langle \downarrow_{q,W} H\rangle \supset H$. Thus, in (5) and (7), matrix P_k should be replaced by $\bar{P}_k = \bar{H}_k\bar{H}_k^T$. This step was omitted by the authors in order to ease the readability of the paper.

B. Optimal controller

Given a zonotopic state estimation $\langle c_k, H_k\rangle$, the idea is to design an optimal state estimate feedback control law $u_k^* = -L_k^*c_k$, such that minimizes the loss function

$$J_N = \mathscr{Q}[\sum_{k=0}^{N-1} x_k^TWx_k + u_k^TUu_k] \tag{8}$$

where W and U are symmetric positive definite matrices of appropriate dimensions.

At a generic instant k and state x_k, the optimal *cost-to-go* is given by

$$V_k(x_k) = \min_{u_k^*,\ldots,u_{N-1}^*} \left\{ \mathscr{Q}[\sum_{j=k}^{N-1} x_j^TWx_j + u_j^TUu_j] \right\} \tag{9}$$

which, following the analogy between the expect value and the operator introduced in (1), can be reformulated as

$$V_k(x_k) = \mathscr{Q}[c_k^TS_kc_k] + s_k \tag{10}$$

with S_k and s_k defined by the recursions

$$S_k = A^T S_{k+1} A + W - A^T S_{k+1} B (B^T S_{k+1} B + U)^{-1} B^T S_{k+1} A \tag{11a}$$

$$s_k = s_{k+1} + Tr[W P_k] + Tr[S_{k+1}(G_k^*(C P_k C^T + Q_v) G_k^{*T})] \tag{11b}$$

and the optimal control action given by

$$u_k^* = -(B^T S_{k+1} B + U)^{-1} B^T S_{k+1} A c_k = -L_k^* c_k \tag{12}$$

with matrix $A - BL_k^*$ Schur stable due to Assumption 1.

From equations (10)-(12), the value of the loss function for a time horizon N is given by

$$\begin{aligned} J_N = V_0(x_0) = \mathscr{Q}[c_0^T S_0 c_0] + Tr[\sum_{k=0}^{N-1} W P_k] + \\ + Tr[\sum_{k=0}^{N-1} S_{k+1}(G_k^*(C P_k C^T + Q_v) G_k^{*T})] \end{aligned} \tag{13}$$

with $\mathscr{Q}[c_0^T S_0 c_0] = c_0^T S_0 c_0$.

C. Stationary conditions

Analogously to the stochastic case, the observer gain converges to the fixed gain

$$G^* = AK^* = AP_\infty C^T (CP_\infty C^T + Q_v)^{-1} \tag{14}$$

with P_∞ the solution of the discrete algebraic Ricatti equation (DARE)

$$P_\infty = AP_\infty A^T + Q_w - AP_\infty C^T (CP_\infty C^T + Q_v)^{-1} CP_\infty A^T \tag{15}$$

Similarly, the controller gain converges at the fixed gain

$$L^* = (B^T S_\infty B + U)^{-1} B^T S_\infty A \tag{16}$$

with S_∞ the solution of the DARE

$$S_\infty = A^T S_\infty A + W - A^T S_\infty B (B^T S_\infty B + U)^{-1} B^T S_\infty A \tag{17}$$

Therefore, the computation of the infinity horizon loss function yields

$$J_\infty = \lim_{N \to \infty} J_N / N = Tr[W P_\infty] + Tr[S_\infty (G^* (CP_\infty C^T + Q_v) G^{*T})] \tag{18}$$

where, taking into consideration (14) and (15), and making use of the trace properties[1], (18) can be rewritten as

$$J_\infty = Tr[(W + A^T S_\infty A - S_\infty) P_\infty] + Tr[S_\infty Q_w] \tag{19}$$

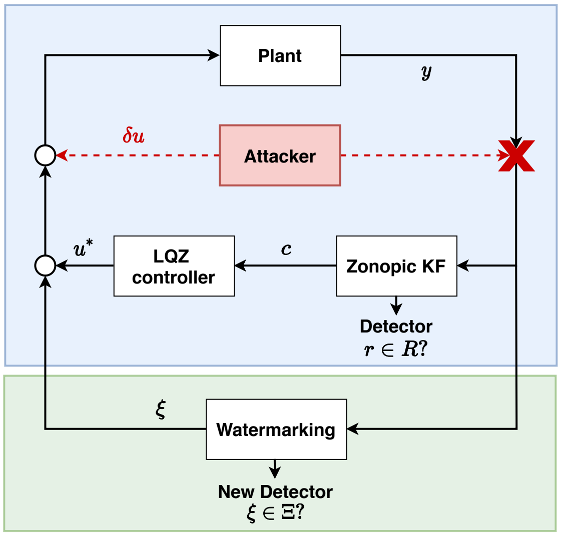

Fig. 1. Overall control/detection scheme

D. Anomalies detector

The operation of the system under consideration is monitored based on the values adopted by the residual vector

$$r_k = y_k - Cc_k = C(x_k - c_k) + Fv_k \tag{20}$$

with $x_k - c_k \in \langle 0, H_k \rangle$. Accordingly, in healthy operation the residual vector satisfies $r_k \in R_k$, with the residual zonotopic set computed as

$$R_k = C\langle 0, H_k \rangle \oplus F\langle 0, I_{n_v} \rangle = \langle 0, [CH_k, \; F] \rangle \tag{21}$$

Since the study of the replay attack focuses in the stationary operation of the system, in the sequel, it will be assumed that the estimation error $x_k - c_k$ is confined within its minimal Robust Positive Invariant (mRPI) set. A zonotopic over-approximation of the mRPI is considered as $\langle 0, H_{inv} \rangle$. Consequently, for the healthy system in the stationary

$$x_k - c_k \in \langle 0, H_{inv} \rangle \tag{22}$$

Furthermore, the residual vector will be confined within the set $R_{inv} = \langle 0, [CH_{inv}, \; F] \rangle$, such that the following reasoning is carried out

$$\begin{cases} r_k \in R_{inv} & \Longrightarrow \text{ Healthy operation} \\ else & \Longrightarrow \text{ Something is wrong} \end{cases} \tag{23}$$

In this regard, the block with blue background in Fig. 1 shows the nominal scheme of the system, where the estimations performed by the ZKF are compared against the sensors measurements in order to elucidate the presence of anomalies in the system operation.

IV. Replay attack characterization

In order to characterize the effect of a replay attack, the following time windows are defined:

1) **Record window:** output data are assumed to be recorded for $K_{rec} = \{k \in \mathbb{N} \; : \; k \in [k_0, \quad k_0 + l - 1]\}$,

[1] The following trace properties hold:

$$Tr[AB] = Tr[BA]$$
$$Tr[ABCD] = Tr[BCDA] = Tr[CDAB] = Tr[DABC]$$

where $l \in \mathbb{N}$ denotes the size of the record window. The set of recorded outputs is $Y_{rec} = \{y_k \ : \ k \in K_{rec}\}$.

2) **Replay window:** real sensors data are replaced for $K_{rep} = \{k \in \mathbb{N} \ : \ k \in [k_1 + (n-1)l, \ k_1 + nl - 1], \forall n \in \{1, ..., n_r\}\}$, where $n_r \in \mathbb{N}^+$ accounts for the total number of repetitions of the recorded sequence.

Let us denote with the superscripts ^{r} and ^{a} the state of the system variables during the record and replay phases, respectively. As an example, for the state variable it follows: $x_k^r = x_k \ \forall k \in K_{rec}$, while $x_k^a = x_k \ \forall k \in K_{rep}$.

In the sequel, it will be assumed that a replay attack launched against the system is undetectable by an anomalies detector like (23). Consequently, despite any possible signal δu injected by the attacker in the system inputs (see Fig. 1), the residuals will satisfy

$$r_k^a \in R_{inv} \quad \forall k \in K_{rep} \tag{24}$$

Aiming to protect this vulnerability, in the next section an exogenous signal policy $\xi_k = f(y_{k-1})$ will be designed such that added to the optimal control action $u_k = u_k^* + \xi_k$ enforces the replay attack detection. In order to introduce such signal, let us define the vector $e_k = x_k - c_k$ such that the closed-loop dynamics of the plant are be expressed as

$$\begin{aligned}\begin{bmatrix} x_{k+1} \\ e_{k+1} \end{bmatrix} &= \begin{bmatrix} A - BL^* & BL^* \\ 0 & A - G^*C \end{bmatrix} \begin{bmatrix} x_k \\ e_k \end{bmatrix} + \begin{bmatrix} B \\ 0 \end{bmatrix} \xi_k + \begin{bmatrix} E & 0 \\ E & -G^*F \end{bmatrix} \begin{bmatrix} w_k \\ v_k \end{bmatrix} \\ y_k &= \begin{bmatrix} C & 0 \end{bmatrix} \begin{bmatrix} x_k \\ e_k \end{bmatrix} + F v_k \end{aligned} \tag{25}$$

By defining the variables $z_k = [x_k^T, \ e_k^T]^T$ and $\alpha_k = [w_k^T, \ v_k^T]^T$, hereinafter, the closed-loop dynamics will be denoted as

$$\begin{aligned} z_{k+1} &= \Phi z_k + \Gamma \xi_k + \Theta \alpha_k \\ y_k &= \Psi z_k + F v_k \end{aligned} \tag{26}$$

V. Detection proposal

This section presents the design of a zonotopically bounded external signal such that enforces the replay attack detection. The signal design is based on the idea of introducing an external disturbance whose dynamics are known by the defender. The effect of this external disturbance is immediately compensated by subtracting the estimation performed by a state observer, in such a way that only the estimation error is injected. A robust zonotopic observer is designed for bounding such error.

According to the aforementioned, let us considered the injection of an exogenous signal $\xi_k \in \mathbb{R}^{n_u}$ composed by

$$\xi_k = \phi - c_k^o \tag{27}$$

where $\phi \in \mathbb{R}^{n_u}$ is a constant vector different from zero $\phi \neq 0$, and $c_k^o \in \mathbb{R}^{n_u}$ is the center of a zonotopic observer that will be introduced later.

A. Signal injection

Constant vector ϕ can be rewritten as

$$\phi = \lambda \phi - (\lambda - 1)\phi$$

for any arbitrarily parameter $\lambda \in \mathbb{R}$. Accordingly, the injection of the exogenous signal (27) in the closed-loop system (26), can be rewritten as follows

$$\begin{bmatrix} z_{k+1} \\ \phi \end{bmatrix} = \begin{bmatrix} \Phi & \Gamma \\ 0 & \lambda I \end{bmatrix} \begin{bmatrix} z_k \\ \phi \end{bmatrix} - \begin{bmatrix} \Gamma c_k^o \\ (\lambda - 1)\phi \end{bmatrix} + \begin{bmatrix} \Theta \\ 0 \end{bmatrix} \alpha_k \tag{28a}$$

$$y_k = \begin{bmatrix} \Psi & 0 \end{bmatrix} \begin{bmatrix} z_k \\ \phi \end{bmatrix} + F v_k \tag{28b}$$

$$\begin{bmatrix} z_0 \\ \phi \end{bmatrix} \in \left\langle \begin{bmatrix} c_0^z \\ c_0^o \end{bmatrix}, H_0^+ \right\rangle \subset \mathbb{R}^{2n_x + n_u} \tag{28c}$$

The introduction of a time-varying gain matrix gain $\mathscr{G}_k$ in (28) yields the equivalent system

$$\begin{aligned} \begin{bmatrix} z_{k+1} \\ \phi \end{bmatrix} &= \begin{bmatrix} \Phi & \Gamma \\ 0 & \lambda I \end{bmatrix} \begin{bmatrix} z_k \\ \phi \end{bmatrix} - \begin{bmatrix} \Gamma c_k^o \\ (\lambda - 1)\phi \end{bmatrix} + \begin{bmatrix} \Theta \\ 0 \end{bmatrix} \alpha_k + \\ &+ \mathscr{G}_k (y_k - \begin{bmatrix} \Psi & 0 \end{bmatrix} \begin{bmatrix} z_k \\ \phi \end{bmatrix} - F v_k) \end{aligned} \tag{29}$$

such that, similar to (4), the zonotope with center and generators matrix defined by

$$\begin{bmatrix} c_{k+1}^z \\ c_{k+1}^o \end{bmatrix} = \left(\begin{bmatrix} \Phi & 0 \\ 0 & \lambda I \end{bmatrix} - \mathscr{G}_k \begin{bmatrix} \Psi & 0 \end{bmatrix} \right) \begin{bmatrix} c_k^z \\ c_k^o \end{bmatrix} - \begin{bmatrix} 0 \\ (\lambda - 1)\phi \end{bmatrix} + \mathscr{G}_k y_k \tag{30a}$$

$$H_{k+1}^+ = \left[\left(\begin{bmatrix} \Phi & \Gamma \\ 0 & \lambda I \end{bmatrix} - \mathscr{G}_k \begin{bmatrix} \Psi & 0 \end{bmatrix} \right) H_k^+, \ \begin{bmatrix} \Theta \\ 0 \end{bmatrix}, \ -\mathscr{G}_k F \right] \tag{30b}$$

satisfies the inclusion property $[z_k^T, \ \phi^T]^T \in \langle [c_k^{zT}, \ c_k^{oT}]^T, H_k^+ \rangle$ $\forall k \geq 0$. Note that the value of the optimal time varying $\mathscr{G}_k^*$ matrix such that minimizes the F-radius of the prediction zonotope can also be designed as explained in Section III-A.

Furthermore, from previous equations it follows

$$\begin{bmatrix} z_k \\ \phi \end{bmatrix} \in \langle \begin{bmatrix} c_k^z \\ c_k^o \end{bmatrix}, H_k^+ \rangle \implies \begin{bmatrix} z_k - c_k^z \\ \phi - c_k^o \end{bmatrix} = \begin{bmatrix} z_k - c_k^z \\ \xi_k \end{bmatrix} \in \langle 0, H_k^+ \rangle \tag{31}$$

and therefore, by defining the projection matrix $M = \begin{bmatrix} 0_{n_u \times 2n_x} & I_{n_u} \end{bmatrix}$, the injected signal satisfies

$$\xi_k \in \Xi_k = M \langle 0, H_k^+ \rangle = \langle 0, M H_k^+ \rangle \tag{32}$$

After a sufficient long time, the estimation error will be ultimately bounded within its mRPI set, for which, a zonotopic over-approximation will be denoted as $\langle 0, H_{inv}^+ \rangle$ and therefore $\Xi_{inv} = \langle 0, M H_{inv}^+ \rangle$.

Moreover, since the value of the constant vector ϕ is known by the defender, signal ξ_k can be used to assess the operation of the system. Accordingly, for the stationary the following reasoning is carried out

$$\begin{cases} \xi_k \in \Xi_{inv} & \implies \text{Healthy operation} \\ else & \implies \text{Something is wrong} \end{cases} \tag{33}$$

Hereinafter, let us define the matrices

$$\mathscr{A}(\lambda) = \begin{bmatrix} \Phi & \Gamma \\ 0 & \lambda I \end{bmatrix} \qquad \mathscr{C} = \begin{bmatrix} \Psi & 0 \end{bmatrix} \tag{34}$$

Remark 2: From the assumption that (A, B) is controllable and (A, C) observable, it follows that the pair $(\mathscr{A}(\lambda), \mathscr{C})$ is observable.

B. Stability of the scheme

If the vector $\tilde{e}_k = [(z_k - c_k^z)^T,\ (\phi - c_k^o)^T]^T$ is introduced. Then, by comparing (28a) with (30a), it can be seen that the dynamics of $\tilde{e}_k$ evolve according to

$$\tilde{e}_{k+1} = (\mathscr{A}(\lambda) - \mathscr{G}_k\mathscr{C})\tilde{e}_k + B_k^\alpha \alpha_k \tag{35}$$

where B_k^α denotes a matrix that gathers the different uncertainty terms.

Consequently, the dynamics of the overall scheme (blue block plus green block in Fig. 1) are

$$\begin{bmatrix} z_{k+1} \\ \tilde{e}_{k+1} \end{bmatrix} = \begin{bmatrix} \Phi & \Gamma M \\ 0 & \mathscr{A}(\lambda) - \mathscr{G}_k\mathscr{C} \end{bmatrix} \begin{bmatrix} z_k \\ \tilde{e}_k \end{bmatrix} + \begin{bmatrix} \Theta \\ B_k^\alpha \end{bmatrix} \alpha_k \tag{36}$$

where Φ (see (25)) is Shur stable, and therefore, the stability of the overall scheme depends on the eigenvalues of the matrix $\mathscr{A}(\lambda) - \mathscr{G}_k\mathscr{C}$.

C. Performance degradation

From (32), the covariation matrix of the zonotope bounding the injected signal can be defined as

$$P_{\xi,k} = MH_k^+(MH_k^+)^T = MH_k^+H_k^{+T}M^T$$

with $P_{\xi,inv} = MH_{inv}^+H_{inv}^{+T}M^T$ for the stationary.

Hence, making use of the analogy between the stochastic and bounded-error fields already presented, the performance loss introduced by the continuous injection of the zonotopically bounded signal ξ_k can be computed as

$$\begin{aligned} J_\infty^\xi = \lim_{N\to\infty} J_N^\xi/N = Tr[WP_\infty] + Tr[S_\infty(G(CP_\infty C^T + Q_v)G^T)] \\ + Tr[(U + B^TS_\infty B)P_{\xi,inv}] = J_\infty + Tr[(U + B^TS_\infty B)P_{\xi,inv}] \end{aligned} \tag{37}$$

for the infinity horizon control problem.

D. Replay attack detection

The standard replay attack in the literature assumes that the attacker records and replays the measurement for the system in steady-state operation. Thus, during the record phase

$$\xi_k^r = \phi - c_k^{o,r} \in \Xi_{inv} \quad \forall k \in K_{rec} \tag{38}$$

On the other hand, during the replay phase, the new residuals can be rewritten as

$$\xi_k^a = \phi - c_k^{o,a} = \phi - c_k^{o,r} + (c_k^{o,r} - c_k^{o,a}) = \xi_k^r + (c_k^{o,r} - c_k^{o,a}) \tag{39}$$

Hence, since ξ_k^r is bounded as expressed in (38), the detectability of the attack will depend on the evolution of the estimation center c^o in between phases. Note that, for the replay phase, the center of the new estimator operates based on the false measurements y_k^r, such that

$$\begin{bmatrix} c_{k+1}^{z,a} \\ c_{k+1}^{o,a} \end{bmatrix} = (\begin{bmatrix} \Phi & 0 \\ 0 & \lambda I \end{bmatrix} - \mathscr{G}^* \begin{bmatrix} \Psi & 0 \end{bmatrix}) \begin{bmatrix} c_k^{z,a} \\ c_k^{o,a} \end{bmatrix} - \begin{bmatrix} 0 \\ (\lambda - 1)\phi \end{bmatrix} + \mathscr{G}^* y_k^r \tag{40}$$

while during the record phase the center of the estimator behave as

$$\begin{bmatrix} c_{k+1}^{z,r} \\ c_{k+1}^{o,r} \end{bmatrix} = (\begin{bmatrix} \Phi & 0 \\ 0 & \lambda I \end{bmatrix} - \mathscr{G}^* \begin{bmatrix} \Psi & 0 \end{bmatrix}) \begin{bmatrix} c_k^{z,r} \\ c_k^{o,r} \end{bmatrix} - \begin{bmatrix} 0 \\ (\lambda - 1)\phi \end{bmatrix} + \mathscr{G}^* y_k^r \tag{41}$$

Consequently, if matrix $\mathscr{G}^*$ is split as $\mathscr{G}^* = \begin{bmatrix} \mathscr{G}_1^T & \mathscr{G}_2^T \end{bmatrix}^T$, then, by comparing (40) and (41), it can be seen that the center difference between phases is governed by the dynamics

$$\begin{bmatrix} c_{k+1}^{z,r} - c_{k+1}^{z,a} \\ c_{k+1}^{o,r} - c_{k+1}^{o,a} \end{bmatrix} = \begin{bmatrix} \Phi - \mathscr{G}_1\Psi & 0 \\ -\mathscr{G}_2\Psi & \lambda I \end{bmatrix} \begin{bmatrix} c_k^{z,r} - c_k^{z,a} \\ c_k^{o,r} - c_k^{o,a} \end{bmatrix} \tag{42}$$

and therefore, by setting the parameter $\lambda > 1$, the dynamics of (42) will diverge causing that the residual ξ_k exits the set Ξ_{inv}, triggering thus the detection of the attack.

Remark 3: Note that the detection speed depends on the value of the parameter λ. However, this value also affects the size of the optimal bounding zonotope Ξ, and hence, according to (37), the value of the performance loss introduced in the system.

Remark 4: In the moment that the signal ξ_k exits the set Ξ_{inv}, the signal stops being injected in order to not affect the system with its exponential growth.

VI. Numerical example

Let us consider a discrete-time LTI system, see (2), with the following system matrices

$$A = \begin{bmatrix} 0.9842 & 0.0407 \\ -0.1327 & 0.9590 \end{bmatrix} \quad B = \begin{bmatrix} 1 & 0.7 \\ 0 & 1.752 \end{bmatrix} \quad C = \begin{bmatrix} 0.3 & 0 \\ 0 & 0.5 \end{bmatrix}$$

besides, the process disturbance and measurements noise input matrices are

$$E = \begin{bmatrix} 0.05 & 0.02 \\ 0 & 0.05 \end{bmatrix} \qquad F = \begin{bmatrix} 0.01 & 0 \\ 0 & 0.01 \end{bmatrix}$$

with the uncertainty variables $w_k, v_k \in \langle 0, I_2 \rangle$.

Previous system is controlled by means of a state estimation based control law where the state observer is a ZKF whose optimal gain matrix in the stationary is

$$G^* = \begin{bmatrix} 2.4847 & 0.2090 \\ -0.2537 & 1.6477 \end{bmatrix}$$

Setting the weighting matrices $W = 10 \cdot I_2$ and $U = I_2$, the stationary value of the optimal LQZ control gain is

$$L^* = \begin{bmatrix} 0.9384 & -0.3006 \\ -0.0550 & 0.5248 \end{bmatrix}$$

and the infinity horizon loss function is $J_\infty = 0.1183$.

A. Signal design

A zonotopically bounded exogenous signal $\xi_k \in \mathbb{R}^2$ for detecting replay attack will be designed for the closed-loop dynamics of the system presented above. In order to design such signal, the constant vector $\phi = [1,\ 1]^T$ will be used and the parameter value λ is set to $\lambda = 1.05$.

Consequently, a robust zonotopic observer of the form (30) is designed such that the computed optimal steady-state gain matrix is

$$\mathscr{G}^* = \begin{bmatrix} 2.288 & -0.146 & 0.396 & -0.077 & 0.562 & -0.011 \\ 0.227 & 1.521 & -0.037 & 0.158 & -0.115 & 0.197 \end{bmatrix}^T$$

A zonotopic over-approximation of the mRPI set for the estimation error of the observer (30) is computed as $\langle 0, H_{inv}^+ \rangle$. Accordingly, by defining the projection matrix $M = [0_{2\times 4}\ I_2]$, for the stationary, the external signal ξ_k satisfies $\xi_k \in \Xi_{inv} = \langle 0, MH_{inv}^{+} \rangle$. For the value of the parameter $\lambda = 1.05$, the induced performance loss with respect the nominal system is $\Delta J = J_{\infty}^{\xi} - J_{\infty} = 0.0322$.

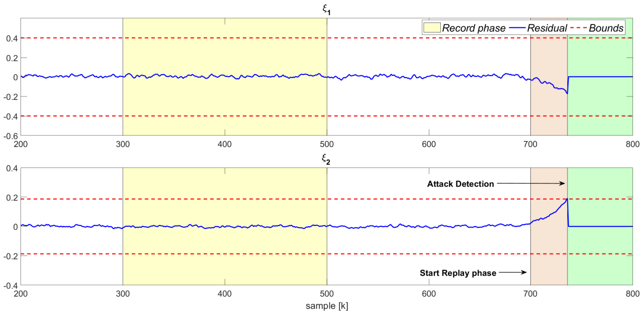

Fig. 2. Signal ξ temporal evolution

B. Replay attack example

In this section, a replay attack scenario is simulated. The attacker is assumed to secretly record the system outputs during the time interval $K_{rec} = [300,\ 500]^T$. Besides, at time $k = 700$, the attacker starts replaying back in a loop the previously recorded data.

Blue lines in Fig. 2 show the temporal evolution of the two components of signal ξ_k during the simulation. Additionally, red dashed lines represent the interval bounds of the zonotopic set Ξ_{inv}. It can be seen how after the start of the replay phase, the signal ξ_k starts growing exponentially until $k = 736$ when one of the components of ξ_k exits the set Ξ_{inv}, and therefore the attack is detected. Note that, after attack detection the signal stops being injected.

Figure 3 plots the temporal evolution of the system outputs throughout the previously described attack scenario. During the nominal operation, it can be seen the small effect that the injection of signal ξ_k has on the system outputs. Since the recorded data is still being replayed back, the stabilization of the system outputs after the attack detection is due to the own dynamics of the plant (matrix A is Schur stable). No stability guarantees can be given in such situation.

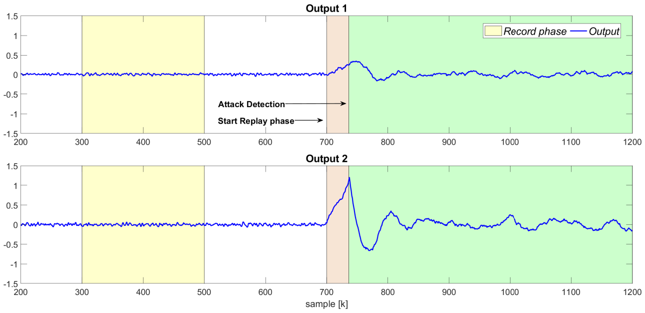

Fig. 3. System outputs temporal evolution

Figure 4 shows the effect of the parameter λ in the existing trade-off between the induced performance loss ΔJ and the detection time. In this regard, the mean detection time was computed running 100 simulations for each value of λ, with a difference in between the values of 0.01.

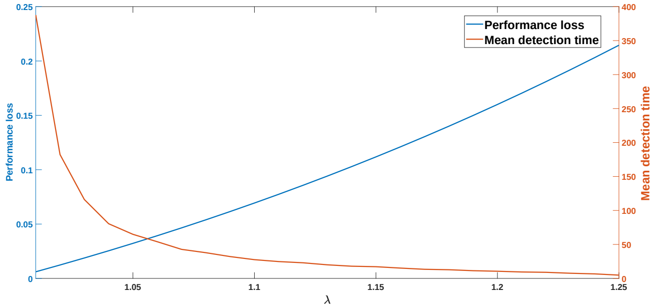

Fig. 4. Parameter comparison

VII. Conclusions

The paper introduces the concept of LQZ controller. This is done with the aim of obtaining a metric that helps to assess the impact on the infinity horizon control problem of the injection of a zonotopically bounded watermarking signal. Besides, the design of a zonotopically bounded external signal such that enforces replay attack detectability is also addressed. In the present work, the design of such watermarking signal was kept as simple as possible, ignoring the optimization of several design parameters that could improve the trade-off between performance loss and detection time. An in-depth study on the specifications of the watermarking signal will be carried out in the future.

References

[1] H. S. Sánchez, D. Rotondo, T. Escobet, V. Puig, and J. Quevedo, "Bibliographical review on cyber attacks from a control oriented perspective," *Annual Reviews in Control*, 2019.

[2] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE transactions on automatic control*, vol. 58, no. 11, pp. 2715–2729, 2013.

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

[4] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *First Workshop on Secure Control Systems (SCS), Stockholm, 2010*, 2010.

[5] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *2009 47th annual Allerton conference on communication, control, and computing*. IEEE, 2009, pp. 911–918.

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

[7] A. Khazraei, H. Kebriaei, and F. R. Salmasi, "A new watermarking approach for replay attack detection in lqg systems," in *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*. IEEE, 2017, pp. 5143–5148.

[8] F. Miao, M. Pajic, and G. J. Pappas, "Stochastic game approach for replay attack detection," in *52nd IEEE conference on decision and control*. IEEE, 2013, pp. 1854–1859.

[9] V. T. H. Le, C. Stoica, T. Alamo, E. F. Camacho, and D. Dumur, *Zonotopes: From guaranteed state-estimation to control*. John Wiley & Sons, 2013.

[10] C. Combastel, "Zonotopes and kalman observers: Gain optimality under distinct uncertainty paradigms and robust convergence," *Automatica*, vol. 55, pp. 265–273, 2015.

[11] ——, "A state bounding observer for uncertain non-linear continuous-time systems based on zonotopes," in *Proceedings of the 44th IEEE Conference on Decision and Control*. IEEE, 2005, pp. 7228–7234.