Security of Control Systems: Prevention of Aging Attacks by means of Convex Robust Simulation Forecasts

Cédric Escudero, Paolo Massioni, Gérard Scorletti, Eric Zamaï

Security of Control Systems: Prevention of Aging Attacks by means of Convex Robust Simulation Forecasts

Cédric Escudero *, **Paolo Massioni** **, **Gérard Scorletti** ***, **Eric Zamaï** **

* *G-SCOP CNRS, Grenoble Institute of Technology, 38000 Grenoble, France (email: cedric.escudero@grenoble-inp.fr).*
** *Laboratoire Ampère CNRS, INSA Lyon, Université de Lyon, 69621 Villeurbanne CEDEX, France (email: {paolo.massioni,eric.zamai}@insa-lyon.fr).*
*** *Laboratoire Ampère CNRS, Ecole Centrale Lyon, Université de Lyon, 69134 Ecully CEDEX, France (email: gerard.scorletti@ec-lyon.fr).*

Abstract: Aging attacks are a class of attacks targeting closed-loop control systems connected to a network. Such attacks consist in slightly modifying the control signals to increase the wear and tear of the physical system while maintaining the delivered service. In this paper, we exploit the technique of robust simulation of linear systems for forecasting and preventing these attacks by means of convex optimization. Besides, this technique allows the computation of the time at which the normal aging is not guaranteed anymore for a given control input set. The paper end highlights an example application upon an electrical machine.

Keywords: Aging attacks, secure control theory, Lyapunov methods, sum of squares, linear matrix inequalities.

1. INTRODUCTION

Modern control systems consist of digital control components, such as controllers and networks, for monitoring and controlling a physical system. With their digitization, they are now suffering from vulnerabilities like any computer-based system. As a result, modern control systems have been the target of attackers (Franck et al., 2018). So, they aim at taking control over the physical system in order to damage it or degrade the control system's performances which might lead to damages. Over the past decade, the physical system integrity has became a major concern for the security of control systems (Escudero et al., 2018). In particular, deception attacks, a type of attacks, have gained attention. They consist in altering the behavior of the physical system by compromising one or multiple control components (e.g. controller, network) (Teixeira et al., 2012).

In the secure control literature, prevention and detection of deception attacks have been investigated from the standpoint of the control system's performances (Giraldo et al., 2018). In other words, they are interested in attacks that alter the control system's objective which is related to the services delivered by the physical system. Mo et al. (2014) investigate the detection and the feasibility of replay attacks in which an attacker manipulates the control signals while replaying a sequence of recorded sensor measurements. Bai et al. (2015) quantify the maximum degradation of the control system's performances an attacker can induce by hijacking and replacing the control signal in the presence of an anomaly detector. With a similar attacker model, Teixeira et al. (2012) exploit the unobservable states in order to mislead the anomaly detector and the controller about the physical system's states. Murguia et al. (2017) analyze the consequences of stealthy attacks over the control system's performances by the means of positively invariant sets. Similarly, Hadizadeh Kafash et al. (2018) propose to limit the positively invariant set to satisfy properties of the physical system's services.

In this work context, we focus on a class of attacks that we call "aging attacks". Their goal is mainly to reduce the physical system's lifetime. They consist in slightly modifying the control signals reaching the actuators to maximize the wear and tear of the machinery, subsequently reducing its lifetime, causing increased corrective maintenance and potential dangers to the attacked party. At the same time, the attacker will make sure that the control system's objective is not degraded for the stealthiness purpose. As aging attack examples, the temperature increase in an electrical machine deteriorates earlier its insulation system which leads further to a failure. Also, the power consumption increase in an autonomous system leads to a fast discharge of the energy storage which ceases its operations.

Aging attacks act on dynamical systems, which makes their forecast and prevention amenable to be dealt with using the methods of systems and control theory. Previous works have been conducted in Escudero and Zamaï (2019) to limit the available actuator output range by the means of positively invariant sets. As a continuation of these

works, we propose in this paper to use robust convex simulation which is less conservative and allows to consider the time dimension. The methodology is based on the ability of forecasting the possible reachable states of the closed-loop plant under an external attack, which allows tuning the actuators range in order to prevent them. The proposed forecasting method is based on Pseudo-Lyapunov function for determining ellipsoidal bounding sets that capture the state trajectory of a dynamical system over a given time interval.

The rest of the paper is organized as follows. Section 2 presents the problem, the attacker model and the main theoretical background. Section 3 gives the main theorem which is sufficient conditions for computing ellipsoidal bounding set over a time interval. Section 4 presents the algorithms for limiting the available actuator output range such that aging attacks cannot be launched. Section 5 highlights our main contributions for preventing attacks on an example application of a brushed DC motor. Finally, concluding remarks and directions are given in Section 6.

2. PRELIMINARIES

2.1 Notation

Let $\mathbb{R}$ be the set of real numbers, and $\mathbb{R}^{n\times m}$ be the set of real $n \times m$ matrices. Given a vector $v \in \mathbb{R}^n$, $v^\intercal$ denotes its transpose, and $[v]_i$ is the i^{th} element of v. Given a matrix A, $A^\top$ indicates its transpose, $diag(a_1, a_2, ..., a_n)$ denotes the diagonal matrix with the diagonal elements $a_1, a_2, ..., a_n$, I_n is the identity matrix of size n, $0_{n,m}$ is the zero matrix of size n, m. The notation $A \succeq 0$ ($A \preceq 0$) indicates the positive (negative) semidefiniteness -i.e. all the eigenvalues of the symmetric matrix A are positive (negative) or equal to zero-, whereas $A \succ 0$ ($A \prec 0$) indicates the positive (negative) definiteness -i.e. eigenvalues are strictly positive (negative).- We also define $\mathcal{E}_v(A, \bar{v})$ as the ellipsoid of dimension n with matrix $A \in \mathbb{R}^{n\times n}$, $A = A^\top \succ 0$ and centered in $\bar{v} \in \mathbb{R}^n$ -i.e. $\mathcal{E}_v(A, \bar{v}) = \{v \in \mathbb{R}^n \,|\, (v - \bar{v})^\top A(v - \bar{v}) \leqslant 1\}$.- In addition, let $\mathcal{H}_v(c, \mu)$ be an hyperplane defined as $\mathcal{H}_v(c, \mu) = \{v \in \mathbb{R}^n \,|\, c^\top v = \mu\}$. Finally, let $\mathbb{R}_m[t]$ be the set of polynomials of degree up to m in the variable t, and $\mathbb{R}^{n\times n}_m[t]$ be the set of symmetric matrix-valued polynomials of degree up to m in the variable t of size $n \times n$, with $m \in \mathbb{N}$.

Physical system: In this paper, we consider dynamical systems modelled as affine time-invariant continuous-time systems as follows:

$$\dot{x}(t) = Ax(t) + Bu(t) + a \tag{1}$$

where $x(t) \in \mathbb{R}^n$ is the state vector, $u(t) \in \mathbb{R}^m$ is the input vector, $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times m}$, and $a \in \mathbb{R}^n$.

The model in (1) above can be simplified by defining the extended state vector $\tilde{x}(t) = [x^\top(t), 1]^\top$, which allows reformulating it as:

$$\dot{\tilde{x}}(t) = \tilde{A}\tilde{x}(t) + \tilde{B}u(t) \tag{2}$$

with

$$\tilde{A} = \begin{bmatrix} A & a \\ 0_{1,n} & 0 \end{bmatrix}, \quad \tilde{B} = \begin{bmatrix} B \\ 0_{1,m} \end{bmatrix}. \tag{3}$$

With this notation, an ellipsoid $\mathcal{E}_x(Q, \bar{x}) = \{x \in \mathbb{R}^n \,|\, (x - \bar{x})^\top Q(x - \bar{x}) \leqslant 1\}$ is equivalently defined by the set $\{\tilde{x} = [x^\top, 1]^\top \,|\, x \in \mathbb{R}^n,\ \tilde{x}^\top \tilde{Q} \tilde{x} \leqslant 1\}$, where

$$\tilde{Q} = \begin{bmatrix} Q & -Q\bar{x} \\ -\bar{x}^\top Q & \bar{x}^\top Q \bar{x} \end{bmatrix} \in \mathrm{R}^{(n+1)\times(n+1)}. \tag{4}$$

Remark 1. Without loss of generality, we consider that in the model in (2) it is possible to distinguish the states related to the service delivered by the physical system x_g, in other words the states involved into the control system's objective, from the states x_s related to the stress of the physical system.

Anomaly detector: Let an output feedback controller satisfy a control system's objective for the physical system's services in (2) such that $(\bar{u}(t), \bar{x}_g(t))$ is a nominal trajectory for the system in (2). In addition, it is reasonable to assume the presence of sensors for monitoring the service such that the controller can comply with the control system's objective. This set of measurement is captured by $y_g(t) \in \mathbb{R}^l$ with $y_g(t) = Cx_g(t)$.

In addition, we consider an anomaly detector that monitors deviations from a nominal trajectory at each time instant from the component-wise absolute value:

$$r_g(t) = |\hat{y}_g(t) - y_g(t)| \tag{5}$$

where $\hat{y}_g(t)$ is the estimated measurement vector, and $r_g(t) \in \mathbb{R}^l$ is the residue vector with each of its component is evaluated to a threshold $\tau\mathbb{R}^l$ for determining the presence of an anomaly as in (6):

$$r_g(t) \leqslant \tau. \tag{6}$$

2.2 Attacker model and problem formulation

Regarding the attack space formulated in Teixeira et al. (2012), we define the attacker model for aging attacks as follows. The attacker is able to inject additional control data in the actuator channel by compromising either the controller or the actuator channel itself which is captured by having $u(t) = \bar{u}(t)+u^a(t)$. However, the attacker cannot eavesdrop on the sensor and actuator data. In other words, the attack policy assumes no online data. In addition, the attack is computed a priori corresponding to an open-loop type of attack policy. The attacker has access to the physical system model in (2) and the anomaly detector model in (5), (6).

Therefore, the attacker's objective consists in searching for a control signal $u^a(t)$ that maximizes the stress states $x_s(t)$ while guaranteeing the service residue $r_g(t)$ remains below the anomaly detector's threshold τ (stealthiness).

In complement, the defender's objective is the prevention of aging attacks formulated as searching for the upper bound of $u(t)$ that maximizes the service states $x_g(t)$ while guaranteeing the stress states remains below a certain theshold corresponding to a normal aging behavior. Clearly, adding additional sensors for monitoring the stress states might be considered, but will inherently increase the attack surfaces allowing an attacker taking advantage of them. That is why we propose to prevent the aging attacks by restricting the control input $u(t)$ received by the physical system.

The rest of the section provides the main theoretical background for understanding the results of this paper.

2.3 Sum of squares

In this paper, we are going to rely on a technique called Sum Of Squares (SOS), which allows casting several classes of polynomial problems into convex optimization problems. We recall here briefly the basic notions that are necessary for understanding the paper, the interested reader can then consult the references that are provided.

Definition 1. (SOS problems, Parrilo (2003)). Let $p(t) \in \mathbb{R}_{2d}[t]$; we call Sum Of Squares problem (SOS) the problem of finding whether there exists a finite number l of polynomials $\pi_i(t) \in \mathbb{R}_d[t]$ such that

$$p(t) = \sum_{i=1}^{l} \pi_i(t)^2. \tag{7}$$

If such an expression exists, then $p(t)$ is a sum of squares (SOS), which implies that $p(t) \geqslant 0$ for all t.

The class above can be extended to the class of Matrix SOS problems (MSOS).

Definition 2. (MSOS problems, Chesi (2010)). Let $\mathcal{P}(t) \in \mathbb{R}_{2d}^{n\times n}[t]$; we call a Matrix Sum Of Squares problem (MSOS) the problem of finding whether there exists a finite number l of matrices of polynomials $\Pi_i(t)$ such that

$$\mathcal{P}(t) = \sum_{i=1}^{l} \Pi_i(t)^\top \Pi_i(t). \tag{8}$$

If such a decomposition exists, then $P(t)$ is a matrix sum of squares (MSOS), which implies that $P(t) \succeq 0$ for all t.

The definitions above are restricted to univariate polynomials, as this is the case we consider in this paper. SOS and MSOS problems are convex problems. A derived class of problems is that of feasibility problems under SOS or MSOS constraints.

Definition 3. (SOS constraints feasibility, Parrilo (2003)). Let $p_i(t,\theta) \in \mathbb{R}_{2d}[t]$, $\forall i \in \{1,2,...,q\}$, where $\theta \in \mathbb{R}^\rho$ is a vector of parameters or unknowns, with $p_i(t,\theta)$ affine with respect to the entries of θ. A feasibility problem under SOS constraints consists in finding, if it exists, a value of $\theta = \theta^*$ for which

$$p_i(t,\theta^*) \text{ is SOS, for } i = 1,...,q. \tag{9}$$

If such a θ^* exists, then the problem is feasible; otherwise it is unfeasible.

Definition 4. (MSOS constraints feasibility, Chesi (2010)). Let $\mathcal{P}_i(t,\theta) \in \mathbb{R}_{2d}^{n\times n}[t]$, $\forall i \in \{1,2,...,q\}$, where $\theta \in \mathbb{R}^\rho$ is a vector of parameters or unknowns, and the matrices $P_i(t,\theta)$ are affine with respect to the entries of θ. A feasibility problem under SOS constraints consists in finding, if it exists, a value of $\theta = \theta^*$ for which

$$P_i(t,\theta^*) \text{ is MSOS, for } i = 1,...,q. \tag{10}$$

If such a θ^* exists, then the problem is feasible; otherwise it is unfeasible.

Feasibility problems under SOS and MSOS problems are convex optimization problems, and they can be reformulated as linear matrix inequality (LMI) feasibility problems; this can either be done explicitly, or relying on automated procedures, like the one available in the Yalmip toolbox (Löfberg, 2009) under Matlab. Minimising any single affine function of the decision variables under SOS and/or MSOS constraints is also a convex optimization problem.

2.4 The generalised S-procedure

The S-procedure allows restricting some classes of inequalities to a certain given subset of the variables that are concerned (Boyd et al., 1994). In this paper, we rely on a general expression which can be specialised according to the cases.

Lemma 1. (Generalised S-procedure). Let $F(x)$, $G(x)$ be (symmetric matrix) functions of the (vector) variable x. Let $g(x)$ be a scalar function of x. The following implications hold.

$$F(x) \succeq 0 \text{ for } G(x) \succeq 0 \Leftarrow F(x) - G(x)\lambda \succeq 0 \text{ for } \lambda \geqslant 0,\ \forall x \tag{11}$$

$$F(x) \succeq 0 \text{ for } g(x) \geqslant 0 \Leftarrow F(x) - g(x)\Lambda \succeq 0 \text{ for } \Lambda \succeq 0,\ \forall x \tag{12}$$

The terms Λ and λ are called multipliers, which can be chosen at one's convenience, i.e. they are decision variables subject to the positivity constraints above. When used in the context of polynomial problems as in this case, the lemma above is a direct consequence of a lemma known as Positivstellensatz (Chesi, 2010) or p-satz, of which several versions exist in the literature. The multipliers can in this case have a polynomial dependence on x, which allows satisfying the positivity constraints by means of either SOS or MSOS constraints.

2.5 Robust simulation and Pseudo-Lyapunov functions

By robust simulation (Kantner and Doyle, 1996) we mean simulation of a dynamical system for a whole set of initial conditions, under a certain number of constraints. Namely, the problem of robust simulation consists in finding a bounding set for the state $x(t)$ at a final time t_f, given a set of possible initial values for it at an initial time t_0; this under the hypotheses of a given dynamical equation and in the presence of additional constraints of different kind. In this work, we consider ellipsoids as bounding sets.

In the context of this work, we adapt the ideas in Ben-Talha et al. (2017); Tobenkin et al. (2011), that are based on the search of a time-dependent pseudo-Lyapunov function. The idea is to define a positive definite function

$$V(\tilde{x}(t),t) = \tilde{x}(t)^\top \tilde{Q}(t)\tilde{x}(t) > 0\ \forall x(t) \neq 0, \tag{13}$$

such that $\dot{V}(\tilde{x}(t),t) \leqslant 0$, where $\tilde{Q}(t)$ is a time-varying symmetric matrix. Then the following lemma holds, under the hypothesis of $u(t) = 0$.

Lemma 2. Consider the system in (2), with initial conditions at t_0 satisfying $\tilde{x}(t_0)^\top \tilde{Q}_{t_0} \tilde{x}(t_0) \leqslant 1$. If there exists a matrix function $\tilde{Q}(t) = \tilde{Q}(t)^\top \in \mathbb{R}^{n\times n}$, with $\tilde{Q}(t_0) = \tilde{Q}_{t_0}$ such that

$$\dot{\tilde{Q}}(t) + \tilde{A}^\top \tilde{Q}(t) + \tilde{Q}(t)\tilde{A} \preceq 0 \text{ for } t \in [t_0, t_f], \tag{14}$$

then $\tilde{x}(t)^\top \tilde{Q}(t)\tilde{x}(t) \leqslant 1$ for $t \in [t_0, t_f]$.

The lemma above can be interpreted as follows: $\tilde{x}(t_0)$ is inside the level curve of value 1 of the function $V(\tilde{x}(t),t)$. The inequality in (14) implies that for all trajectories of

the state according to (2), the function can only decrease; so those trajectories are bounded to stay inside the same level curve at all times $t \in [t_0, t_f]$.

3. MAIN THEOREM

The main theoretical result of this paper consists in a theorem providing sufficient conditions for computing the ellipsoidal bounding set over a time interval $[t_0, t_f]$ for a system as in (1). This theorem will be subsequently employed in a set of algorithms, whose goal is the prediction and prevention of potential aging attacks.

The main theorem is obtained by generalising Lemma 2 in order to account for the presence of a bounded input signal. In fact, we will assume $u(t) \in \mathcal{E}_u(R, \bar{u})$, i.e.

$$(u - \bar{u})^\top R(u - \bar{u}) \leqslant 1 \tag{15}$$

with $R \in \mathbb{R}^{m\times m}$ a symmetric matrix, for which we assume $R \succ 0$.

In the presence of input, the time derivative of the pseudo-Lyapunov function $V(x(t), t)$ defined in (13) is not (14), but it becomes:

$$\dot{V}(x(t), t) = \begin{bmatrix}\tilde{x}(t)\\ u(t)\end{bmatrix}^\top \begin{bmatrix}\dot{\tilde{Q}}(t) + \tilde{A}^\top\tilde{Q}(t) + \tilde{Q}(t)\tilde{A} & \tilde{Q}(t)\tilde{B}\\ \tilde{B}^\top\tilde{Q}(t) & 0_{m,m}\end{bmatrix}\begin{bmatrix}\tilde{x}(t)\\ u(t)\end{bmatrix}. \tag{16}$$

Notice that if $\dot{V}(x(t), t) \leqslant 0$, then $V(\tilde{x}(t), t)$ defines time-variant ellipsoidal level sets from which the state trajectory will never go out over the given time interval; so if a set of initial conditions is within a level curve, the trajectories stemming from them will never exit the level curve of the same value. The time-variant $\tilde{Q}(t)$ allows the ellipsoidal level curves to move and grow or shrink over time with the state trajectory, whether they are converging or not.

In order to make the search tractable, we are going to limit it to the set of matrix-valued polynomials, i.e. we will set $\tilde{Q}(t) \in \mathbb{R}_{2d}^{(n+1)\times(n+1)}[t]$ for an arbitrarily chosen integer $d \geqslant 1$. It is clear that specifying $\tilde{Q}(t)$ in this way adds some conservatism, which can be progressively reduced by increasing the degree of the matrix-valued polynomial. $\dot{\tilde{Q}}(t)$ is then its first time-derivative, with $\dot{\tilde{Q}} \in \mathbb{R}_{2d-1}^{(n+1)\times(n+1)}[t]$.

As the attacker wants to remain stealthy regarding the anomaly detector, we may assume that the control signals will be chosen carefully in order to not degrade the service delivered by the physical system. For this reason, we can assume that a part of the state can be constrained to belong to a given specific set, the set that will not cause any suspects of attack to arise. This ellipsoid will be defined as $\mathcal{E}_x(\Xi, \xi)$, where Ξ in general will be rank-deficient (it will basically only constrain x_g), as it will constrain only one part of the state; $\mathcal{E}_x(\Xi, \xi)$ can even coincide with $\mathbb{R}^{n\times n}$ (formally by picking $\Xi = 0$). As a consequence of this, we formulate the following assumption:

Assumption 1. There exists an input signal $u(t) \in \mathcal{E}_u(R, \bar{u})$ such that $x(t) \in \mathcal{E}_x(\Xi, \xi)$ for any $t \in [t_0, t_f]$ and for initial conditions $x(t_0) \in \mathcal{E}_x(Q(t_0), \bar{x}(t_0))$.

If the assumption above is not satisfied, it means that no aging attack can be performed without being detected, which put us on the safe side.

Finally, just before formulating our main result, we define three additional terms which will be useful later on. First, it will be necessary at some steps to extract the term 1 from $\tilde{x}$, for which we define

$$\Gamma = [0_{1,n}\ 1] \tag{17}$$

such that $\Gamma\tilde{x} = 1$. Subsequently, we can also define

$$\gamma(t) = (t_f - t)(t - t_0), \tag{18}$$

which allows expressing the constraint of $t \in [t_0, t_f]$ equivalently as simply $\gamma(t) \geqslant 0$. Last, consider

$$\tilde{I} = \begin{bmatrix}I_n & 0_{n,1}\\ 0_{1,n} & 0\end{bmatrix}, \tilde{\Xi} = \begin{bmatrix}\Xi & 0_{n,1}\\ 0_{1,n} & 0,\end{bmatrix}, \tilde{\xi} = \begin{bmatrix}\xi\\ 0\end{bmatrix}. \tag{19}$$

We can now formulate the main theorem.

Theorem 1. Consider an affine time-invariant continuous-time system according to (1) or equivalently (2), with matrices defined according to (3).

If for a given $d \geqslant 1$ there exist $\tilde{Q}(t) \in \mathbb{R}_{2d}^{(n+1)\times(n+1)}[t]$, $Z(t), X(t) \in \mathbb{R}_{2d-2}^{(n+1)\times(n+1)}[t]$ $\alpha(t), \beta(t) \in \mathbb{R}_{2d-2}[t]$, and a scalar $\varepsilon > 0$ for which the following constraints are satisfied:

$$-M(t) - \alpha(t)S - \beta(t)T - \gamma(t)Z(t) \text{ is MSOS}, \tag{20}$$

$$\tilde{Q}(t) - \gamma(t)X(t) - \varepsilon\tilde{I} \text{ is MSOS} \tag{21}$$

$$Z(t),\ X(t) \text{ are MSOS} \tag{22}$$

$$\alpha(t), \beta(t) \text{ are SOS} \tag{23}$$

with

$$M(t) = \begin{bmatrix}\dot{\tilde{Q}}(t) + \tilde{A}^\top\tilde{Q}(t) + \tilde{Q}(t)\tilde{A} & \tilde{Q}(t)\tilde{B}\\ \tilde{B}^\top\tilde{Q}(t) & 0_{m,m}\end{bmatrix}$$

$$S = \begin{bmatrix}\Gamma^\top\Gamma - \Gamma^\top\bar{u}^\top R\bar{u}\Gamma & \Gamma^\top\bar{u}^\top R\\ R\bar{u}\Gamma & -R\end{bmatrix}$$

$$T = \begin{bmatrix}\Gamma^\top\Gamma - \tilde{\Xi} + \tilde{\Xi}\tilde{\xi}\Gamma + \Gamma^\top\tilde{\xi}^\top\tilde{\Xi} - \Gamma^\top\tilde{\xi}^\top\tilde{\Xi}\tilde{\xi}\Gamma & 0_{n+1,m}\\ 0_{m,n+1} & 0_{m,m}\end{bmatrix}$$

and Γ, $\gamma(t)$, $\tilde{I}$ defined as in (17), (18), (19), then

$$\tilde{x}(t_0)^\top\tilde{Q}(t_0)\tilde{x}(t_0) \leqslant 1 \Rightarrow \tilde{x}(t)^\top\tilde{Q}(t)\tilde{x}(t) \leqslant 1\ \forall t \in [t_0, t_f], \tag{24}$$

under the constraints $\forall t \in [t_0, t_f] u(t) \in \mathcal{E}_u(R, \bar{u})$, $x(t) \in \mathcal{E}_x(\Xi, \xi)$.

Proof. Consider first (21); left and right multiply by $\tilde{x}(t)$, and consider $\gamma(t)X(t)$ as an S-procedure term by positive multiplier $X(t)$ as in (22); this implies (Lemma 1):

$$\tilde{x}(t)^\top\tilde{Q}(t)\tilde{x}(t) \geqslant \varepsilon||x(t)||^2 \tag{25}$$

when $\gamma(t) \geqslant 0$, i.e. $V(x(t), t) = \tilde{x}(t)^\top\tilde{Q}(t)\tilde{x}(t) > 0$ when $x(t) \neq 0$, $t \in [t_0, t_f]$. Subsequently, consider (20); left and right multiply by $[\tilde{x}(t)^\top, u(t)^\top]^\top$, and consider $\alpha(t)S$, $\beta(t)T$ and $\gamma(t)Z(t)$ as S-procedure terms by positive multipliers $\alpha(t)$, $\beta(t)$ and $Z(t)$ as in (22) and (23); this implies (Lemma 1):

$$[\tilde{x}(t)^\top, u(t)^\top]\, M(t)\, [\tilde{x}(t)^\top, u(t)^\top]^\top = \dot{V}(x(t), t) \leqslant 0 \tag{26}$$

when

$$[\tilde{x}(t)^\top, u(t)^\top]\, S\, [\tilde{x}(t)^\top, u(t)^\top]^\top \geqslant 0 \Leftrightarrow u(t) \in \mathcal{E}_u(R, \bar{u}). \tag{27}$$

$$[\tilde{x}(t)^\top, u(t)^\top]\, T\, [\tilde{x}(t)^\top, u(t)^\top]^\top \geqslant 0 \Leftrightarrow x(t) \in \mathcal{E}_x(\Xi, \xi), \tag{28}$$

and when $\gamma(t) \geqslant 0$, i.e. when $t \in [t_0, t_f]$. This means that the value of $V(x(t), t)$ can only increase under the stated constraints, i.e. $V(x(t_0), t_0) \leqslant 1 \Rightarrow V(x(t), t) \leqslant 1$ in the considered interval, which is the theorem statement.

Remark 2. Although SOS problems are exact for the univariate case, Theorem 1 is conservative, i.e. it provides sufficient but not necessary conditions, for two main reasons: 1) the pseudo-Lyapunov function is constrained to be of a specific form, and 2) the use of the generalized S-procedure for obtaining (20). In both cases the conservatism can be reduced by increasing d, which provides more degrees of freedom to the function, as well as it reduces the conservatism of the S-procedure according to the applicable formulation of the p-satz Lasserre (2015). Notice also that the polynomial degrees of $\tilde{Q}(t)$, $Z(t)$, $X(t)$, $\alpha(t)$, and $\beta(t)$ have all been chosen in order to have all terms in (20) of the same degree; in fact, the overall cost of solving the MSOS problem depends on the overall degree in t of the expression in (20), so it is computationally inefficient to have terms of the sum of higher degree with respect to the others. In other words, the conservatism is minimum for a given computational cost when all terms have the same degree.

4. ALGORITHMS FOR ATTACK ANALYSIS AND PREVENTION

In this section, we are proposing algorithms involving Theorem 1 for preventing aging attacks over a given time interval. In other words, we want to restrain the input set $\mathcal{E}_u(R, \bar{u})$ into the set $\mathcal{E}_u(\hat{R}, \bar{u})$ ($\mathcal{E}_u(\hat{R}, \bar{u}) \subseteq \mathcal{E}_u(R, \bar{u})$) such that a dangerous set $\mathcal{D}_x$ is avoided over a time interval $[t_0, t_f]$.

Firstly, we are interested in finding the minimal bouding ellipsoid for the system defined in (1) over the time interval $[t_0, t_f]$. In fact, there exists many bounding ellipsoids under Theorem 1; however, we want to find the tighest ellipsoid set that encapsulates the state trajectory over the time interval. This can be obtained by maximizing the trace of $\tilde{Q}(t_f)$ under Theorem 1 with initial conditions ($Q(t_0)$,$\bar{x}(t_0)$) as stated in $\mathbf{P_1}$. In order to give more degrees of freedom to the search of such ellipsoids and without loss of generality, let t_0 be time 0 and split the final time t_f in $N \in \mathbb{N}$ time steps such that $N = t_f \Delta_t^{-1}$ with Δ_t a small time step, which simplifies the computations. Hence, Algorithm 1 is proposed for finding the minimal bounding ellipsoid for system in (2) with a control input set $\mathcal{E}_u(R, \bar{u}))$ over the time interval $[0, \Delta_t]$ by using Theorem 1.

$$\mathbf{P_1}: \quad \underset{\tilde{Q}_t, Z(t), X(t), \alpha(t), \beta(t)}{\text{maximize}} \quad \text{trace}(\tilde{Q}_{\Delta_t}) \qquad \text{subject to} \quad (20), (21), (22), (23)$$

Notice that the numerical procedure will have a limited numerical precision, for this reason a normalisation step (step 3.) has been introduced; typically the ellipsoids matrices might not fit into the form of (4), with a non-matching lower-right entry that corresponds to defining a set $\{v \in \mathbb{R}^n \,|\, (v-\bar{v})^\top A^{nn}(v-\bar{v}) \leqslant \rho\}$ with $\rho \neq 1$. The function Normalize($\tilde{A}^{nn}$) transforms a non-normalized (nn) ellipsoid defined as $\mathcal{E}_v^{nn}(A^{nn}, \bar{v}) = \{v \in \mathbb{R}^n \,|\, (v-\bar{v})^\top A^{nn}(v-\bar{v}) \leqslant \rho\}$ into a normalized one $\mathcal{E}_v(A, \bar{v})$ ($\rho = 1$).

Algorithm 1 : $[Q_{\Delta_t}, \bar{x}_{\Delta_t}]$=Alg1($Q(t_0)$,$\bar{x}(t_0)$,$R$,$\bar{u}$,$\Xi$,$\xi$, $\mathbf{I_1}$)

Input: $Q(t_0)$,$\bar{x}(t_0)$,R,$\bar{u}$, Ξ, ξ, $\mathbf{I_1}$:=$\{A,\ B,\ \Delta_t,\ d\}$
Initial condition: $Q_0 = Q(t_0)$, $\bar{x}_0 = \bar{x}(t_0)$
1. Set $\tilde{Q}_0 = \begin{bmatrix} Q_0 & -Q_0\bar{x}_0 \\ -\bar{x}_0^\top Q_0 & \bar{x}_0^\top Q_0 \bar{x}_0 \end{bmatrix}$,
$\tilde{Q}(t) = \sum_{i=0}^{2d} \tilde{Q}_i t^i$
2. Solve $\mathbf{P_1}$
3. $[Q(\Delta_t), \bar{x}(\Delta_t)]$=Normalize($\tilde{Q}(\Delta_t)$)
Output: $Q(\Delta_t)$, $\bar{x}(\Delta_t)$

Secondly, we propose Algorithm 2, whose goal is to determine if and at which time $t_\cap$ (with $t_\cap \in \{0, \Delta_t, ..., N\Delta_t\}$) the bounding ellipsoid hits a dangerous set $\mathcal{D}_x$. We consider the dangerous set as a set where the lifetime for the given system is reduced.

Consider the dangerous set as the union of i number of halfspaces $\mathcal{H}_x^i(c_i, \mu_i)$ defined by their boundary hyperplane in (29):

$$\mathcal{D}_x = \{x \in \mathbb{R}^n : \bigcup_{i=1}^{p} c_i^\top x(t) \geq \mu_i\} \tag{29}$$

where $c_i \in \mathbb{R}^n$ is an affine combination of states in x, $\mu_i \in \mathbb{R}$ is the bound. Let us formulate the overlapping distance from an ellipsoid $\mathcal{E}_v(A, \bar{v})$ to an hyperplane $\mathcal{H}_v^i(c_i, \mu_i)$ denoted dist($\mathcal{E}_v(A, \bar{v}), \mathcal{H}_v^i(c_i, \mu_i)$) detailed in Kurzhanskiy and Varaiya (2006) as follows:

$$\text{dist}(\mathcal{E}_v(A, \bar{v}), \mathcal{H}_v^i(c_i, \mu_i)) = \frac{(c_i^\top A^{-1} c_i)^{1/2} - |\mu_i - c_i^\top \bar{v}|}{(c_i^\top c_i)^{1/2}} \tag{30}$$

where dist($\mathcal{E}_v(A, \bar{v}), \mathcal{H}_v(c, \mu)) \geqslant 0$ if the ellipsoid hits the hyperplane -i.e. the ellipsoid intersects the hyperplane-; otherwise it is negative. Hence, for determining if an ellipsoid $\mathcal{E}_v(A, \bar{v})$ hits a dangerous set $\mathcal{D}_x$ in (29), it is sufficient to verify that the distance from the ellipsoid to each hyperplane is negative, leading to the boolean function Hit(A,$\bar{v}$,$\mathcal{H}_v^i$).

Algorithm 2 : [hit, $t_\cap$]=Alg2($Q(t_0)$,$\bar{x}(t_0)$,R,$\bar{u}$,Ξ,ξ, $\mathbf{I_1}$,$\mathbf{I_2}$)

Input: $Q(t_0)$,$\bar{x}(t_0)$,R,$\bar{u}$,Ξ,ξ, $\mathbf{I_1}$,$\mathbf{I_2}$:= $\{\mathcal{H}_x^i,\ t_f\}$
Initial condition: $Q_0 = Q(t_0)$, $\bar{x}_0 = \bar{x}(t_0)$
1. Set $N = t_f \Delta_t^{-1}$
2. For $j = 1$ to N
  2.1. $[Q_{\Delta_t}, \bar{x}_{\Delta_t}]$=Alg1($Q_0$,$\bar{x}_0$,$R$,$\bar{u}$,$\Xi$,$\xi$, $\mathbf{I_1}$,$\mathbf{I_2}$)
  2.2. If Hit(Q_{Δ_t},$\bar{x}_{\Delta_t}$,$\mathcal{H}_x^i$) = $True$
    Set $hit = True$, $t_\cap = j\Delta_t$, Goto Output
  2.3. Set $Q_0 = Q_{\Delta_t}$, $\bar{x}_0 = \bar{x}_{\Delta_t}$
3. Set $hit = False$, $t_\cap = \emptyset$
Output: hit, $t_\cap$

Finally, Algorithm 3 aims at restraining the input set to the set $\mathcal{E}_u(\hat{R}, \bar{u})$ such that the given dangerous set is guaranteed to be unreachable by the state trajectory for system in (1) over the time interval [0,t_f]. The algorithm implements a bisection method on the scaling term δ for R for solving the quasi-convex problem. Note that higher the trace of R is, tighter the constraints on $u(t)$ are.

Algorithm 3 converges, with respect to a tolerance tol, to the minimal restrained input set $\mathcal{E}_u(\hat{R}, \bar{u})$ with $\hat{R} = \delta R_0$ for a sufficiently large R_0 such that the dangerous set is not reachable by the state trajectory for $\mathcal{E}_u(R_0, \bar{u})$, and a $\underline{\delta} \in [0, 1]$ sufficiently small such that the state trajectory can reach the dangerous set for $\mathcal{E}_u(\underline{\delta} R_0, \bar{u})$.

Algorithm 3 :[$diag$, δ_{wrk}]= Alg3(R_0,$\underline{\delta}$,tol,$Q(t_0)$,$\bar{x}(t_0)$,$\bar{u}$,Ξ,ξ, $\mathbf{I_1}$,$\mathbf{I_2}$)

Input: R_0,$\underline{\delta}$,tol,$Q(t_0)$,$\bar{x}(t_0)$,$\bar{u}$,Ξ,ξ, $\mathbf{I_1}$,$\mathbf{I_2}$
Initial condition: $diag = NotFound$, $Q_0 = Q(t_0)$, $\bar{x}_0 = \bar{x}(t_0)$
1. Set $\overline{\delta} = 1$
2. [hit, $t_\cap$]=Alg2($Q(t_0)$,$\bar{x}(t_0)$,$\underline{\delta} R_0$,$\bar{u}$,Ξ,ξ,$\mathbf{I_1}$,$\mathbf{I_2}$)
3. If $hit = False$
   3.1. Set $diag = NeverHit$, $\delta = \underline{\delta}$, Goto Output
4. [hit, $t_\cap$]=Alg2($Q(t_0)$,$\bar{x}(t_0)$,$\overline{\delta} R_0$,$\bar{u}$,Ξ,ξ,$\mathbf{I_1}$,$\mathbf{I_2}$)
5. If $hit = True$
   5.1 Set $diag = AlwaysHit$, $\delta = \emptyset$, Goto Output
6. Set $\delta = \overline{\delta}$
7. While $(\overline{\delta} - \underline{\delta} > tol)$
   7.1. $\delta_{it} = (\overline{\delta} + \underline{\delta})/2$
   7.2. $R = \delta_{it} R_0$
   7.3. [hit, $t_\cap$]=Alg2($Q(t_0)$,$\bar{x}(t_0)$,R,$\bar{u}$,Ξ,ξ,$\mathbf{I_1}$,$\mathbf{I_2}$)
   7.4. If $hit = True$, Set $\underline{\delta} = \delta_{it}$
   7.4. Else, Set $\overline{\delta} = \delta_{it}$, $diag = Found$, $\delta = \delta_{it}$
Output: $diag$, δ

5. APPLICATION

In this section, we propose to apply the proposed algorithms for a brushed DC motor by first analyzing the potential aging an attacker can induce from the power supply limits, and lastly preventing them.

5.1 Description of the system

Consider a brushed DC motor from Salah and Abdelati (2009) with a constant load torque $T_l = 0.5$ given in (31) controlled by an output feedback controller issuing a voltage $u(t)$ through a network to its armature for achieving a control objective on its angular velocity $\omega(t)$ (service); consider also a single aging factor, which is the winding temperature increase $\theta(t)$. Regarding the lifetime, we assume a normal aging behavior given for $\theta(t) \leq \theta_n$. For the sake of simplicity, we consider $\theta(t) = k_{DC} i^2(t)$ with $k_{DC} = 0.34$ the DC gain of the thermal model which leads to $-i_n \leqslant i(t) \leqslant i_n$ with $i_n = 21.6$ A for guaranteeing the lifetime. Hence, the dangerous set $\mathcal{D}_x$ is defined for $\mathcal{H}_x^1(c_1, \mu_1)$ and $\mathcal{H}_x^2(c_2, \mu_2)$ with $c_1 = [0, 1]^\top$, $\mu_1 = 21.6$, $c_2 = [0, -1]^\top$, $\mu_2 = -21.6$. Recall that the control signal reaching the brushed DC motor is expressed as $u(t) = \bar{u}(t) + u^a(t)$ with $\bar{u}(t)$ the nominal control input and $u^a(t)$ the attack signal. The state-space matrices of the system are:

$$A = \begin{bmatrix} -0.72 & 31.97 \\ -17.64 & -29.31 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 9.62 \end{bmatrix}, \quad a = \begin{bmatrix} -8.71 \\ 0 \end{bmatrix}, \tag{31}$$

with the state vector $x(t) = [\omega(t), i(t)]^\top$.

In both the coming example applications, we have considered $\tilde{Q}(t)$ MSOS of degree 4 ($d = 2$), $Z(t), X(t)$ a matrix (MSOS of degree 0), and $\alpha(t)$ SOS of degree 4, and $\beta(t)$ an unknown scalar (SOS of degree 0).

5.2 Attack analysis: forecast simulation

In this subsection, we analyze the potential aging an attacker can induce to the brushed DC motor from the power supply limits. The control input set can be defined as $R = \frac{1}{u_{bnd}^2}$ which is maximal (R_{max}) -i.e. in the sense of its size- for $u_{bnd} = 110$ V and $\bar{u} = 0$ from the power supply limits. From this maximal control input set, we want to verify if the physical integrity of the brushed DC motor -i.e. aging- can be transgressed over the time interval $[t_0, t_f]$. Instead of stopping the simulation once a bounding ellipsoid at time $t = j\Delta_t$ in Algorithm 2 hits with the dangerous set, we stop it once the bounding ellipsoids converge, in this case for $t_f = 1s$. We apply Algorithm 2 with the inputs: $R = \frac{1}{110^2}$, $\bar{u} = 0$, $Q(t_0) = diag(10^5, 10^7)$, $\bar{x}(t_0) = [0, 0]^\top$, $\Xi = 0$, $\xi = [0, 0]^\top$, $\Delta_t = 0.1$ ms, $t_f = 1$ s. The result is graphically shown in Fig. 1 for each bounding ellipsoids at each 10 ms.

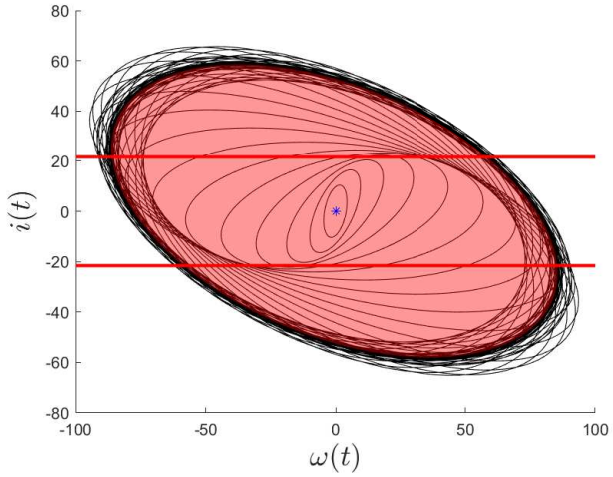

Fig. 1. Bounding ellipsoids at each 10 ms for $t_f = 1$ s from initial conditions $\mathcal{E}_x(diag(10^5, 10^7), [0, 0]^\top)$ (blue star) and $\mathcal{E}_u(\frac{1}{110^2}, 0)$; final bounding ellipsoid (filled ellipsoid in red) ; boundaries of the dangerous set (red lines).

The bounding ellipsoid hits for the first time the dangerous set at $t_\cap = 34.9$ ms. From this analysis, we can note that the physical system can reach the dangerous set over the given time interval [0,1s]. As a result, an attacker is capable to induce an anomalous aging to the brushed DC motor by injecting an attack signal $u^a(t)$.

5.3 Prevention of attacks

In this subsection, we want to restrain the control input set such that the dangerous set can never be hit. We apply Algorithm 3 on the previous example for finding the maximal restrained control input set such that none of the bounding ellipsoids hits the dangerous set over the given time interval. The inputs are: $R_0 = \frac{1}{30^2}$, $\underline{\delta} = 0.01$, $tol = 0.01$, $Q(t_0) = diag(10^5, 10^7)$, $\bar{x}(t_0) = [0, 0]^\top$, $\bar{u} = 0$, $\Xi = 0$, $\xi = [0, 0]^\top$, $\Delta_t = 0.1$ ms, $t_f = 1$ s. The restrained

control input set $\mathcal{E}_u(\hat{R}, \bar{u})$ is given from the output $\delta = 0.6674$ of Algorithm 3 and computed as $\hat{R} = \delta R_0 = \frac{1}{36.72^2}$.

The resulting bounding ellipsoids over the time interval [0,1 s] for the restrained control input set $\mathcal{E}_u(\hat{R}, \bar{u})$ computed in Algorithm 3 are shown for each 10ms in Fig.2.

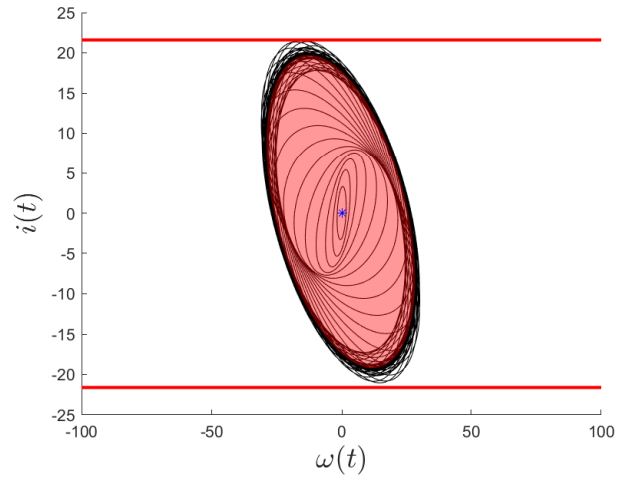

Fig. 2. Bounding ellipsoids at each 10 ms for $t_f = 1$ s from initial conditions $\mathcal{E}_x(diag(10^5, 10^7), [0,0]^\top)$ (blue star) and $\mathcal{E}_u(\frac{1}{36.72^2}, 0)$; final bounding ellipsoid (filled ellipsoid in red) ; boundaries of the dangerous set (red lines).

As we can see in Fig.2, the dangerous set is guaranteed unreachable for $u(t) \in \mathcal{E}_u(\frac{1}{36.72^2}, 0)$. Therefore, aging attacks are prevented by restricting the control input $u(t)$ to the restrained input set.

In Fig.3, it is represented the bounding ellipsoids evolution with respect to the time $t \in [0, 1$ s] for the maximal control input set $\mathcal{E}_u(\frac{1}{110^2}, 0)$ computed in the previous subsection (transparency) and the restrained control input set $\mathcal{E}_u(\frac{1}{36.72^2}, 0)$ (non transparent).

Secondly, we want to prevent stealthy aging attacks that might occur while the system trajectory is constant and given for $(\bar{u}, \bar{x})$ with $\bar{u} = 20$ and $\bar{x} = [10.07, 0.5]^\top$. The attacker aims at remaining stealthy regarding the anomaly detector in (5) tuned at $\tau = 20$ by ensuring the states related to the service lie into $\mathcal{E}_x(\Xi, \xi)$ with $\Xi = diag(\frac{1}{\tau^2}, 0)$ and $\xi = \bar{x}$. Applying Algorithm 3 with $R0 = \frac{1}{1^2}$, $\underline{\delta} = 0.01$, $tol = 0.1$, and $Q(t_0) = diag(10^5, 10^7)$, $x(t_0) = \bar{x}$, it yields the restrained input set $\mathcal{E}_u(\frac{1}{3.1^2}, 20)$. The resulting bounding ellipsoids at each 20 ms are given in Fig.4. As we can observe in Fig.4, the bounding ellipsoids never hit the dangerous set for the computed restrained input set. This ensures for the constant nominal trajectory to prevent aging attacks.

Finally, we compute the evolution of the time at which the normal aging is not guaranteed anymore with respect to the evolution of the restrained input set. In other words, we compute the hit time $t_\cap$ in function of δu_{bnd} with $\delta \in [0, 1]$ from Algorithm 2 with the following inputs: $R = \frac{1}{(\delta u_{bnd})^2}$, $\bar{u} = 0$, $Q(t_0) = diag(10^5, 10^7)$, $\bar{x}(t_0) = [0,0]^\top$, $\Xi = 0$, $\xi = [0,0]^\top$, $\Delta_t = 0.1$ ms, $t_f = 1$ s. The resulting curve is shown in Fig. 5. It represents the secured zone in which

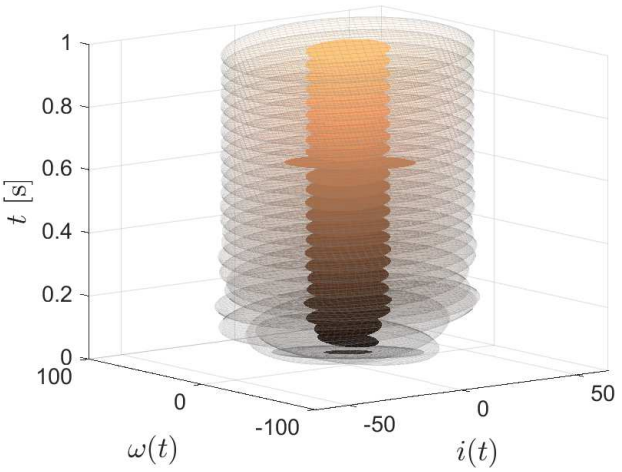

Fig. 3. Bounding ellipsoids evolution from initial conditions $\mathcal{E}_x(diag(10^5, 10^7), [0,0]^\top)$ with respect to the time t for $t_f = 1$ s at each 40 ms for $\mathcal{E}_u(\frac{1}{110^2}, 0)$ (transparent) and for $\mathcal{E}_u(\frac{1}{36.72^2}, 0)$ (non-transparent)

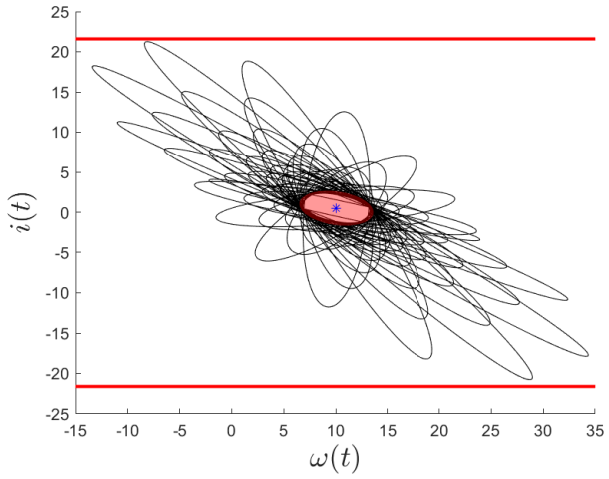

Fig. 4. Bounding ellipsoids at each 20 ms for $t_f = 1$ s from initial conditions $\mathcal{E}_x(diag(10^5, 10^7), [10.07, 0.5]^\top)$ (blue star) and $\mathcal{E}_u(\frac{1}{3.1^2}, 20)$, $\Xi = diag(\frac{1}{20^2}, 0)$, $\xi = [10.07, 0.5]^\top$; final bounding ellipsoid (filled ellipsoid in red) ; boundaries of the dangerous set (red lines).

the normal aging is guaranteed. This curve is computed from Algorithm 2 for different values of δ.

We can observe that the hit time increases with the decrease of the size of the control input set. Hence, the lower the upper bound of $u(t)$, the longer is the period of time in which the normal aging is guaranteed. In addition, from a certain value of δ the dangerous set is not reachable for any time $t \geq 0$ for the state trajectory of the brushed DC motor. The corresponding $\hat{R}$ is the one obtained previously ($\hat{R} = \frac{1}{36.72^2}$) with the results shown in Fig.2.

6. CONCLUSION

In this paper, we have shown how it is possible to use convex robust simulation for forecast and prevention of

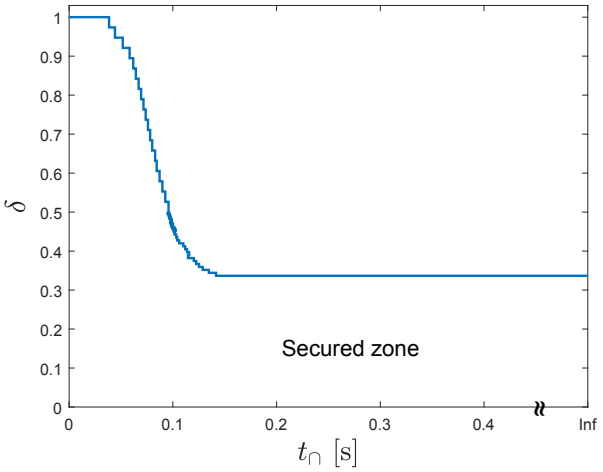

Fig. 5. Secured zone: control input set with $R = \frac{1}{(\delta u_{bnd})^2}$ in function of the hit time $t_\cap$ with $t_f = 1$ s, initial conditions $\mathcal{E}_x(diag(10^5, 10^7), [0, 0]^\top)$ and $\mathcal{E}_u(R, 0)$.

aging attacks. This paper has introduced this new idea and it has presented some preliminary results on a model of brushed DC motor on a very simple attack benchmark, but we can envisage several extensions as topics of future research. First of all, we have considered as the only means of attack prevention the time-invariant restriction of the control input set, but in principle this can be made time-varying, allowing for less restrictive set. Further research will also investigate more deeply the practical application of the methodology to industrial plants.

REFERENCES

Bai, C., Pasqualetti, F., and Gupta, V. (2015). Security in stochastic control systems: Fundamental limitations and performance bounds. In *2015 American Control Conference (ACC)*, 195–200.

Ben-Talha, H., Massioni, P., and Scorletti, G. (2017). Robust simulation of continuous-time systems with rational dynamics. *International Journal of Robust and Nonlinear Control*, 27(16), 3097–3108.

Boyd, S., El Ghaoui, L., Feron, E., and Balakrishnan, V. (1994). *Linear matrix inequalities in system and control theory*, volume 15. SIAM.

Chesi, G. (2010). LMI techniques for optimization over polynomials in control: a survey. *IEEE Transactions on Automatic Control*, 55(11), 2500–2510.

Escudero, C., Sicard, F., and Zamai, E. (2018). Process-aware model based IDSs for industrial control systems cybersecurity: Approaches, limits and further research. In *2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA)*, volume 1, 605–612.

Escudero, C. and Zamaï, E. (2019). Prevention of aging attacks: Malicious nature of the control signal. In *2019 International Automatic Control Conference (CACS)*, 1–6.

Franck, S., Cédric, E., Eric, Z., and Jean-Marie, F. (2018). From ICS attacks' analysis to the S.A.F.E. approach: Implementation of filters based on behavioral models and critical state distance for ICS cybersecurity. In *2018 2nd Cyber Security in Networking Conference (CSNet)*, 1–8.

Giraldo, J., Urbina, D., Cardenas, A., Valente, J., Faisal, M., Ruths, J., Tippenhauer, N.O., Sandberg, H., and Candell, R. (2018). A survey of physics-based attack detection in cyber-physical systems. *ACM Comput. Surv.*, 51(4), 76:1–76:36.

Hadizadeh Kafash, S., Hashemi, N., Murguia, C., and Ruths, J. (2018). Constraining attackers and enabling operators via actuation limits. In *2018 IEEE Conference on Decision and Control (CDC)*, 4535–4540.

Kantner, M. and Doyle, J. (1996). Robust simulation and nonlinear performance. In *35th IEEE Conference on Decision and Control*, volume 3, 2622–2623. IEEE.

Kurzhanskiy, A.A. and Varaiya, P. (2006). *Ellipsoidal Toolbox*. EECS Department, University of California, Berkeley, Tech. Rep.

Lasserre, J. (2015). *An introduction to polynomial and semi-algebraic optimization*, volume 52. Cambridge University Press.

Löfberg, J. (2009). Pre- and post-processing sum-of-squares programs in practice. *IEEE Transactions on Automatic Control*, 54(5), 1007–1011.

Mo, Y., Chabukswar, R., and Sinopoli, B. (2014). Detecting integrity attacks on scada systems. *IEEE Transactions on Control Systems Technology*, 22(4), 1396–1407.

Murguia, C., van de Wouw, N., and Ruths, J. (2017). Reachable sets of hidden cps sensor attacks: Analysis and synthesis tools. *IFAC-PapersOnLine*, 50(1), 2088 – 2094. 20th IFAC World Congress.

Parrilo, P. (2003). Semidefinite programming relaxations for semialgebraic problems. *Mathematical programming*, 96(2), 293–320.

Salah, M. and Abdelati, M. (2009). Parameters identification of a permanent magnet DC motor. volume 675, 177–183.

Teixeira, A., Shames, I., Sandberg, H., and Johansson, K.H. (2012). Revealing stealthy attacks in control systems. In *2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 1806–1813.

Teixeira, A., Pérez, D., Sandberg, H., and Johansson, K.H. (2012). Attack models and scenarios for networked control systems. In *Proceedings of the 1st International Conference on High Confidence Networked Systems*, HiCoNS '12, 55–64. ACM, New York, NY, USA.

Tobenkin, M.M., Manchester, I.R., and Tedrake, R. (2011). Invariant funnels around trajectories using sum-of-squares programming. *IFAC Proceedings Volumes*, 44(1), 9218–9223.