8-2018

State Measurement Spoofing Prevention through Model Predictive Control Design

Helen Durand
Wayne State University, helen.durand@wayne.edu

Recommended Citation

Durand, H., "State Measurement Spoofing Prevention through Model Predictive Control Design," *Proceedings of the 6th IFAC Conference on Nonlinear Model Predictive Control*, 643-648, Madison, Wisconsin, 2018. DOI: 10.1016/j.ifacol.2018.11.034.

State Measurement Spoofing Prevention through Model Predictive Control Design ⋆

Helen Durand *

* *Department of Chemical Engineering and Materials Science, Wayne State University, Detroit, MI 48202, USA (e-mail: helen.durand@wayne.edu).*

Abstract: Security of chemical process control systems against cyberattacks is critical due to the potential for injuries and loss of life when chemical process systems fail. A potential means by which process control systems may be attacked is through the manipulation of the measurements received by the controller. One approach for addressing this is to design controllers that make manipulating the measurements received by the controller in any meaningful fashion very difficult, making the controllers a less attractive target for a cyberattack of this type. In this work, we develop a model predictive control (MPC) implementation strategy that incorporates Lyapunov-based stability constraints and can allow several potential control laws to be available to apply to the process, one of which can be randomly selected at each sampling time, potentially making the response of the controller to a false state measurement more difficult to predict *a priori*. We investigate closed-loop stability and recursive feasibility of the resulting control design, and utilize a benchmark chemical process example to demonstrate the difference in the control actions computed by such a randomized MPC implementation strategy compared with those for the same process by the same MPC design utilized at every sampling time.

Keywords: Cybersecurity, model predictive control, process control.

1. INTRODUCTION

In recent years, cyberattackers have targeted a petrochemical plant (Perlroth and Krauss, 2018), a wastewater treatment plant (Clark et al., 2017), and a uranium enrichment plant (Langner, 2011). Chemical process safety relies on the controllers and safety system to prevent accidents. However, if a cybersecurity breach occurs in a process control system, it may no longer be available to prevent accidents. Even worse, it may be utilized to drive the process state to an unsafe condition that it would not otherwise approach. Randomization has been considered as a cyberattack prevention technique (through, for example, changing network settings (Chavez et al., 2015) or randomly selecting encrypted data from sensors to compare with the information received by operators (Linda et al., 2013)). Due to the criticality of cybersecurity (Smith, 2013) from a safety perspective, it is a topic of significant interest with respect to process control systems. For example, (Rosich et al., 2013) discussed a method for detecting an attack on a controller where it is assumed that the attacker is able to adjust the controller outputs. (Cárdenas et al., 2011) analyzes the potential for an unsafe state to be reached in a system in which the measurements received by a controller are compromised. The present work takes an approach to cybersecurity that uses a randomly selected control law at every sampling time to make the outcome of a cyberattack difficult to predict and therefore to seek to reduce the desirability of performing such attacks. Specifically, we utilize a model predictive control approach that takes advantage of Lyapunov-based stability theory in the design of the constraints to ensure that among all control laws which may be randomly selected at a given sampling time, all will maintain closed-loop stability and be feasible if selected. A chemical process example demonstrates that this randomized controller implementation strategy can maintain closed-loop stability of a nonlinear process operated under the control design and create very different trajectories for the states and inputs than would be observed if one controller was utilized.

⋆ Financial support from Wayne State University is gratefully acknowledged.

2. PRELIMINARIES

2.1 Notation

The notation $|\cdot|$ denotes the Euclidean norm of a vector. A function $\alpha : [0, a) \to [0, \infty)$ is of class $\mathcal{K}$ if $\alpha(0) = 0$ and α is strictly increasing. The notation x^T represents the transpose of a vector x. The symbol " / " denotes set subtraction (i.e., $x \in A/B = \{x \in R^n : x \in A, x \notin B\}$).

2.2 Class of Systems

The class of nonlinear systems under consideration is:

$$\dot{x}(t) = f(x(t), u(t), w(t)) \tag{1}$$

where f is taken to be a locally Lipschitz nonlinear vector function of the state vector $x \in X \subset R^n$, input vector $u \in U \subset R^m$, and disturbance vector $w \in W \subset R^l$, where $W := \{w \in R^l : |w| \leq \theta\}$. We consider that $f(0, 0, 0) = 0$ and assume that the system of Eq. 1 is stabilizable in the sense that there exist explicit stabilizing control laws $h_i(x)$

with corresponding sufficiently smooth positive definite Lyapunov functions $V_i : R^n \to R_+$, and functions $\alpha_{j,i}$, $j = 1, \ldots, 4$, of class $\mathcal{K}$ such that the following inequalities hold for all $x \in D_i \subset R^n$:

$$\alpha_{1,i}(|x|) \leq V_i(x) \leq \alpha_{2,i}(|x|) \tag{2a}$$

$$\frac{\partial V_i(x)}{\partial x} f(x, h_i(x), 0) \leq -\alpha_{3,i}(|x|) \tag{2b}$$

$$\left|\frac{\partial V_i(x)}{\partial x}\right| \leq \alpha_{4,i}(|x|) \tag{2c}$$

$$h_i(x) \in U \tag{2d}$$

for $i = 1, \ldots, n_p$, where D_i is an open neighborhood of the origin. We define a level set of V_i contained within D_i where $x \in X$ as a stability region Ω_{ρ_i} of the nominal ($w(t) \equiv 0$) system of Eq. 1 under the controller $h_i(x)$ ($\Omega_{\rho_i} := \{x \in X \cap D_i : V_i(x) \leq \rho_i\}$). It holds that:

$$|f(x_1, u, w) - f(x_2, u, 0)| \leq L_x|x_1 - x_2| + L_w|w| \tag{3a}$$

$$\left|\frac{\partial V_i(x_1)}{\partial x} f(x_1, u, w) - \frac{\partial V_i(x_2)}{\partial x} f(x_2, u, 0)\right| \leq L'_{x,i}|x_1 - x_2| + L'_{w,i}|w| \tag{3b}$$

$$|f(x, u, w)| \leq M \tag{3c}$$

for all $x, x_1, x_2 \in \Omega_{\rho_i}$, $i = 1, \ldots, n_p$, $u \in U$, and $w \in W$, where $L_x > 0$, $L_w > 0$, and $M > 0$ are selected so that Eqs. 3a and 3c hold regardless of the value of i.

2.3 Lyapunov-based Model Predictive Control

Lyapunov-based model predictive control (LMPC) (Heidarinejad et al., 2012; Mhaskar et al., 2006) is given by:

$$\min_{u(t) \in S(\Delta)} \quad \int_{t_k}^{t_{k+N}} L_e(\tilde{x}(\tau), u(\tau))\, d\tau \tag{4a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0) \tag{4b}$$

$$\tilde{x}(t_k) = x(t_k) \tag{4c}$$

$$\tilde{x}(t) \in X, \, \forall \, t \in [t_k, t_{k+N}) \tag{4d}$$

$$u(t) \in U, \, \forall \, t \in [t_k, t_{k+N}) \tag{4e}$$

$$V_1(\tilde{x}(t)) \leq \rho_{e,1}, \;\; \forall \, t \in [t_k, t_{k+N}), \text{ if } x(t_k) \in \Omega_{\rho_{e,1}} \tag{4f}$$

$$\frac{\partial V_1(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0) \leq \frac{\partial V_1(x(t_k))}{\partial x} f(x(t_k), h_1(x(t_k)), 0) \text{ if } x(t_k) \in \Omega_{\rho_1}/\Omega_{\rho_{e,1}} \tag{4g}$$

where $u(t) \in S(\Delta)$ signifies that the input trajectories are members of the class of piecewise-constant vector functions with period Δ. The nominal (i.e., $w(t) \equiv 0$) model of Eq. 1 (Eq. 4b) is utilized by the LMPC of Eq. 4 to develop predictions $\tilde{x}$ of the process state, starting at a measurement at t_k (Eq. 4c), which are then used in computing the value of the stage cost L_e over the prediction horizon of N sampling periods (Eq. 4a) and evaluating the state constraints (Eq. 4d). The inputs are required to meet the input constraint (Eq. 4e). Eq. 4f requires that the computed inputs maintain the predicted state within the set $\Omega_{\rho_{e,1}}$ throughout the prediction horizon, and Eq. 4g requires that the closed-loop state move toward a neighborhood of the origin. $\Omega_{\rho_{e,1}}$ is chosen to make Ω_{ρ_1} forward invariant under the LMPC of Eq. 4. $h(\tilde{x}(t_q))$, $q = k, \ldots, k+N-1$, $t \in [t_q, t_{q+1})$, is a feasible solution to the optimization problem of Eq. 4 at every sampling time if $x(t_k) \in \Omega_{\rho_1}$. Furthermore, the LMPC of Eq. 4 is guaranteed to maintain the closed-loop state within Ω_{ρ_1} when $\rho_{e,1}$, Δ, and θ are sufficiently small (Heidarinejad et al., 2012). Additionally, V decreases along the closed-loop state trajectory throughout a sampling period when Eq. 4g is activated at t_k.

3. RANDOMIZED LMPC DESIGN

The LMPC design of Eq. 4 computes inputs using a deterministic process model and a limited number of constraints, so that a cyberattacker who knew the control law of Eq. 4 might be able to predict what input might be computed by the controller for a given state measurement $x(t_k)$ and thereby effectively gain control over the process actuators by manipulating the value of $x(t_k)$ received by the controller. Potentially, a cyberattacker could then adjust $x(t_k)$ to apply control actions to the process that he or she believes will cause harm from a safety or economics viewpoint. One method for trying to prevent a cyberattacker from gaining control over the actuators in this manner would be to seek to prevent the cyberattacker from understanding how a given value of $x(t_k)$ may impact the inputs computed by the controller, making it difficult for the attacker to achieve his or her goals and thereby discouraging attacks of this type. An idea for achieving this is to develop a set of controllers that maintain closed-loop stability for a process, and to allow one of these to be randomly selected at every sampling time, potentially preventing a cyberattacker from being able to map a value of $x(t_k)$ to a single process input.

3.1 Randomized LMPC Formulation

Motivated by these considerations, we propose the development of n_p controllers with the following form:

$$\min_{u(t) \in S(\Delta)} \quad \int_{t_k}^{t_{k+N}} L_e(\tilde{x}(\tau), u(\tau))\, d\tau \tag{5a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0) \tag{5b}$$

$$\tilde{x}(t_k) = x(t_k) \tag{5c}$$

$$\tilde{x}(t) \in X, \, \forall \, t \in [t_k, t_{k+N}) \tag{5d}$$

$$u(t) \in U, \, \forall \, t \in [t_k, t_{k+N}) \tag{5e}$$

$$V_i(\tilde{x}(t)) \leq \rho_{e,i}, \;\; \forall \, t \in [t_k, t_{k+N}), \text{ if } x(t_k) \in \Omega_{\rho_{e,i}} \tag{5f}$$

$$\frac{\partial V_i(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0) \leq \frac{\partial V_i(x(t_k))}{\partial x} f(x(t_k), h_i(x(t_k)), 0) \text{ if } x(t_k) \in \Omega_{\rho_i}/\Omega_{\rho_{e,i}} \text{ or } \delta = 1 \tag{5g}$$

where V_i, $\rho_{e,i}$, ρ_i, and h_i, $i = 1, \ldots, n_p$, play the roles in Eq. 5 of V_1, $\rho_{e,1}$, ρ_1, and h_1, respectively, from Eq. 4. Each combination of V_i and h_i is assumed to satisfy Eq. 2 $\forall x \in \Omega_{\rho_i}$ and $\Omega_{\rho_{e,i}} \subset \Omega_{\rho_i}$. For $j = 2, \ldots, n_p$, the Ω_{ρ_j} should be subsets of Ω_{ρ_1} for reasons that will be clarified in Section 3.3. To introduce an additional aspect of randomness at each sampling time, the parameter δ is introduced in Eq. 5g. It can take a value of either 0 or 1, and one of those two values is randomly selected for it at each sampling time. $\delta = 1$ corresponds to activation of the constraint of Eq. 5g even when $x(t_k) \in \Omega_{\rho_{e,i}}$.

3.2 Randomized LMPC Implementation Strategy

With the n_p controllers of the form of Eq. 5 and the two possible values of δ in each of these LMPC's at every sampling time, Eq. 5 represents $2n_p$ potential controllers which may be selected at every sampling time. One could consider other potential control options in addition, such as the Lyapunov-based controllers $h_i(x)$, $i = 1, \ldots, n_p$. However, though all of these controllers are designed and are available in principle, they could cause closed-loop stability issues that require that not all of them be available to be randomly selected between at each sampling time. The conditions which determine which controllers are possibilities at a given sampling time should rely on the position of $x(t_k)$ in state-space and specifically whether $x(t_k) \in \Omega_{\rho_i}$ for the $i-th$ controller to be considered as a candidate. To exemplify this, consider the two level sets Ω_{ρ_1} and Ω_{ρ_2} and their subsets $\Omega_{\rho_{e,1}}$ and $\Omega_{\rho_{e,2}}$ shown in Fig. 1. Two potential values of $x(t_k)$ are presented (x_a and x_b) to exemplify the role that the state-space location of $x(t_k)$ should play in determining which of the n_p controllers of the form of Eq. 5 or the Lyapunov-based controllers of the form $h_i(x(t_k))$ should be considered as candidates to randomly select between at a given sampling time. Consider first that $x(t_k) = x_a$. In this case, $x(t_k) \in \Omega_{\rho_1}/\Omega_{\rho_{e,1}}$, and therefore, as described in Section 2.3, the LMPC of Eq. 5 with $i = 1$ would be able to maintain the closed-loop state in Ω_{ρ_1} throughout the subsequent sampling period. It is also true that $x(t_k) \notin \Omega_{\rho_{e,2}}$, so it may at first seem reasonable to consider that if the LMPC of Eq. 5 is used with $i = 2$, the constraint of Eq. 5g could be activated to decrease the value of the Lyapunov function between two sampling periods and thereby drive the closed-loop state toward the origin using the properties of the Lyapunov-based controller and the constraint of Eq. 5g. However, the closed-loop stability properties delivered by the constraint of Eq. 5g are developed with the requirement that Eq. 2 must hold within the stability region and that $x(t_k)$ must be in this stability region. When $x(t_k) \notin \Omega_{\rho_2}$, these properties are not guaranteed to hold. Therefore, when $x(t_k) = x_a$ in Fig. 1, the LMPC of Eq. 5 with $i = 2$ would not be a wise choice to randomly select at a given sampling time. Similarly, $h_2(x(t_k))$ is guaranteed to maintain closed-loop stability when $x(t_k) \in \Omega_{\rho_2}$, but if $h_2(x(t_k))$ is applied when $x(t_k) = x_a$, $x(t_k) \notin \Omega_{\rho_2}$ and therefore the stability properties are not guaranteed to hold.

In contrast, consider the potential initial condition $x(t_k) = x_b$. In this case, $x(t_k) \in \Omega_{\rho_1}$ and Ω_{ρ_2}. Consequently, Eq. 5 with $i = 1$ or $i = 2$ (for $\delta = 1$ or $\delta = 0$), $h_1(x(t_k))$, and $h_2(x(t_k))$ can all maintain closed-loop stability of the process of Eq. 1, and therefore all could be considered as potential control designs between which to randomly select at t_k. This indicates that the location of $x(t_k)$ in state-space should be checked with respect to Ω_{ρ_i}, $i = 1, \ldots, n_p$, before developing a candidate set of controllers to randomly select between at t_k. However, if Ω_{ρ_i}, $i = 2, \ldots, n_p$, are subsets of Ω_{ρ_1}, then at each sampling time, Eq. 5 with $i = 1$ and $\delta = 0$, Eq. 5 with $i = 1$ and $\delta = 1$, and $h_1(x(t_k))$ are all candidate controllers that can maintain closed-loop stability. If $x(t_k)$ is in the intersection of additional level sets, there are additional candidate controllers which could be randomly selected between.

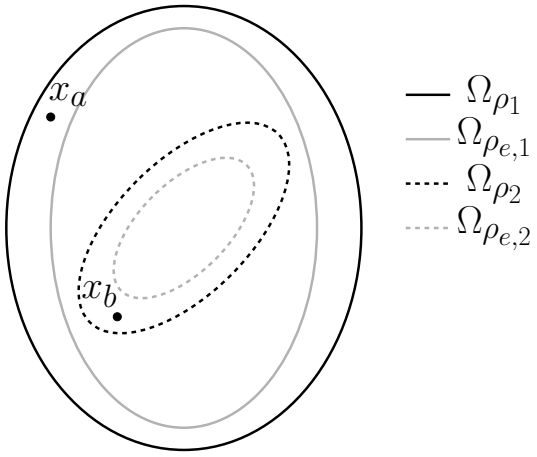

Fig. 1. Intersecting stability regions with two different potential initial conditions $x(t_k) = x_a$ and $x(t_k) = x_b$.

Therefore, the minimum number of candidate controllers is 3, with more potentially being possible, especially as more stability regions with more intersections are developed.

Accounting for the above considerations, the following implementation strategy for the LMPC of Eq. 5 is proposed:

Step 1. At t_k, a random integer j between 1 and $2n_p$ is selected, and δ is randomly selected to be zero or one.

Step 2. If $j \in \{2, \ldots, n_p\}$, set $i = j$. If $j \in \{n_p+2, \ldots, 2n_p\}$, set $i = j - n_p$. Verify that $V_i(x(t_k)) \in \Omega_{\rho_i}$. If yes, move to Step 3. If not, return to Step 1.

Step 3. If j is a number between 1 and n_p, utilize the LMPC of Eq. 5 with $i = j$ and the selected value of δ. If $j = n_p + d$, $d = 1, \ldots, n_p$, set $u = h_d(x(t_k))$.

Step 4. Apply the control action to the process of Eq. 1.

Step 5. $t_k \leftarrow t_{k+1}$. Return to Step 1.

3.3 Randomized LMPC Stability Analysis

In this section, we present the results regarding closed-loop stability of the nonlinear process of Eq. 1 operated under the implementation strategy in Section 3.2 and the feasibility of any LMPC of Eq. 5 selected for determining control actions via this strategy, beginning with two propositions that are utilized in proving the main results.

Proposition 1. (Mhaskar et al., 2013; Heidarinejad et al., 2012) Consider the systems

$$\dot{x}_a(t) = f(x_a(t), u(t), w(t)) \tag{6a}$$

$$\dot{x}_b(t) = f(x_b(t), u(t), 0) \tag{6b}$$

with initial states $x_a(t_0) = x_b(t_0) \in \Omega_{\rho_1}$. There exists a function f_W of class $\mathcal{K}$ such that:

$$|x_a(t) - x_b(t)| \leq f_W(t - t_0) \tag{7}$$

for all $x_a(t), x_b(t) \in \Omega_{\rho_1}$ and all $w(t) \in W$ with:

$$f_W(\tau) = \frac{L_w \theta}{L_x}(e^{L_x \tau} - 1) \tag{8}$$

Proposition 2. (Mhaskar et al., 2013; Heidarinejad et al., 2012) Consider the Lyapunov function $V_i(\cdot)$ of the system of Eq. 1. There exists a quadratic function $f_{V,i}(\cdot)$ such that:

$$V_i(x) \leq V_i(\hat{x}) + f_{V,i}(|x - \hat{x}|) \tag{9}$$

for all $x, \hat{x} \in \Omega_{\rho_i}$ with

$$f_{V,i}(s) = \alpha_{4,i}(\alpha_{1,i}^{-1}(\rho_i))s + M_{v,i}s^2 \tag{10}$$

where $M_{v,i} > 0$ is a constant.

Proposition 3. (Muñoz de la Peña and Christofides, 2008) Consider the Lyapunov-based controller $h_i(x)$ that meets Eq. 2 with Lyapunov function $V_i(\cdot)$, applied in sample-and-hold to the system of Eq. 1. If $\rho_i > \rho_{e,i} > \rho_{\min,i} > \rho_{s,i}$, and $\theta > 0$, $\Delta > 0$, and $\epsilon_{w,i} > 0$ satisfy:

$$-\alpha_{3,i}(\alpha_{2,i}^{-1}(\rho_{s,i})) + L'_{x,i}M\Delta + L'_{w,i}\theta \leq -\epsilon_{w,i}/\Delta \tag{11}$$

then $\forall x(t_k) \in \Omega_{\rho_i}/\Omega_{\rho_{s,i}}$,

$$V_i(x(t)) \leq V_i(x(t_k)) \tag{12}$$

for $t \in [t_k, t_{k+1})$ and $x(t) \in \Omega_{\rho_i}$. Furthermore, if $\rho_{\min,i}$ is defined as follows:

$$\rho_{\min,i} = \max\{V_i(x(t+\Delta)) : V_i(x(t)) \leq \rho_{s,i}\} \tag{13}$$

then the closed-loop state is ultimately bounded in $\Omega_{\rho_{\min,i}}$ in the sense that:

$$\limsup_{t\to\infty} |x(t)| \in \Omega_{\rho_{\min,i}} \tag{14}$$

Theorem 4. Consider the system of Eq. 1 in closed-loop under the implementation strategy of Section 3.2 based on controllers $h_i(x)$ that satisfy Eq. 2, and consider that the conditions in Proposition 3 hold. Let $\epsilon_{w,i} > 0$, $\Delta > 0$, $\rho_i > \rho_{e,i} > \rho_{\min,i} > \rho_{s,i}$ satisfy:

$$\rho_{e,i} \leq \rho_i - f_{V,i}(f_W(\Delta)) \tag{15}$$

and Eqs. 11 and 13, for $i = 1, \ldots, n_p$, and $\Omega_{\rho_{e,j}} \subset \Omega_{\rho_{e,1}}$, $j = 2, \ldots, n_p$. If $x(t_0) \in \Omega_{\rho_1}$ and $N \geq 1$, then the state $x(t)$ of the closed-loop system is always bounded in Ω_{ρ_1}.

Proof. The proof consists of two parts related to 1) characterizable control actions and 2) closed-loop stability.

Part 1. To demonstrate that an input with characterizable properties is returned by the implementation strategy of Section 3.2 at every sampling time to be applied to the process, we note that one of two inputs is returned at every sampling time: a) a control action computed by the LMPC of Eq. 5 with $i = j$ where $x(t_k) \in \Omega_{\rho_j}$ or b) a Lyapunov-based controller $h_j(x(t_k))$ where $x(t_k) \in \Omega_{\rho_j}$.

In case a), a solution to the LMPC of Eq. 5 must have the characterizable property that it met the constraints of the LMPC because the LMPC always has at least one feasible solution. Specifically, $h_i(\tilde{x}(t_q))$, $q = k, \ldots, k+N-1$, $t \in [t_q, t_{q+1})$, with $i = j$, is a feasible solution to the optimization problem of Eq. 5 when $x(t_k) \in \Omega_{\rho_j}$. It causes the constraint of Eq. 5d to be met because $h_i(\tilde{x}(t_q))$, $q = k, \ldots, k+N-1$, $t \in [t_q, t_{q+1})$, maintains the closed-loop state in $\Omega_{\rho_j} \subseteq \Omega_{\rho_1}$ by Proposition 3, and the state constraint of Eq. 5d is met for all states in Ω_{ρ_1}. $h_i(x)$ in sample-and-hold also satisfies the input constraint of Eq. 5e by Eq. 2d. From Proposition 3, it causes the constraint of Eq. 5f to be met when $x(t_k) \in \Omega_{\rho_j}$, and it trivially satisfies the constraint of Eq. 5g. Notably, the feasibility of $h_i(x)$ in sample-and-hold is true regardless of whether $\delta = 1$ or $\delta = 0$ because this is a feasible solution to all constraints of the optimization problem.

In case b), the control action applied to the process is also characterizable because it meets Proposition 3. Therefore, the control action applied at t_k has characterizable properties which can be used in establishing closed-loop stability. Furthermore, whenever Eq. 5 is utilized to determine an input at a given sampling time, a feasible solution to this optimization problem always exists because it is ensured that $x(t_k) \in \Omega_{\rho_i}$ before the solution is obtained, and the feasibility of $h_i(\tilde{x}(t_q))$, $q = k, \ldots, k+N-1$, $t \in [t_q, t_{q+1})$ was demonstrated to hold above as long as $x(t_k) \in \Omega_{\rho_i}$.

Part 2. In this part, we prove that even with a control law randomly selected at every sampling time according to the implementation strategy in Section 3.2, the closed-loop state is maintained within Ω_{ρ_1} for all times if $x(t_0) \in \Omega_{\rho_1}$. To demonstrate this, we first consider the case that at t_k, a control law of the form of Eq. 5 with $i = j$ when $x(t_k) \in \Omega_{\rho_j}$ is selected. In this case, either the constraint of Eq. 5f is activated (if $x(t_k) \in \Omega_{\rho_{e,i}}$), the constraint of Eq. 5g is activated (if $x(t_k) \in \Omega_{\rho_i}/\Omega_{\rho_{e,i}}$ or $\delta = 1$), or both are activated (for example, if $\delta = 1$ but $x(t_k) \in \Omega_{\rho_{e,i}}$).

Consider first the case that Eq. 5f is activated so that from Proposition 2 (assuming that $x(t) \in \Omega_{\rho_i}$ for $t \in [t_k, t_{k+1})$):

$$V_i(x(t)) \leq V_i(\tilde{x}(t)) + f_{V,i}(|x(t) - \tilde{x}(t)|) \tag{16}$$

for $t \in [t_k, t_{k+1})$. With Eq. 5f and Proposition 1, we obtain:

$$V_i(x(t)) \leq \rho_{e,i} + f_{V,i}(f_W(\Delta)) \tag{17a}$$

for $t \in [t_k, t_{k+1})$. When Eq. 15 holds, $V_i(x(t)) \leq \rho_i$, for $t \in [t_k, t_{k+1})$, which validates the assumption used in deriving this result and guarantees that $x(t) \in \Omega_{\rho_i}$ for $t \in [t_k, t_{k+1})$ when $x(t_k) \in \Omega_{\rho_{e,i}}$ and the LMPC of Eq. 5 is used to determine the input to the process of Eq. 1. Because $\Omega_{\rho_i} \subseteq \Omega_{\rho_1}$, $x(t) \in \Omega_{\rho_1}$ for $t \in [t_k, t_{k+1})$.

Consider now the case that Eq. 5g is activated. In this case, we have from this constraint and Eq. 2b that

$$\begin{aligned}&\frac{\partial V_i(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0)\\ &\leq \frac{\partial V_i(x(t_k))}{\partial x} f(x(t_k), h_i(x(t_k)), 0) \leq -\alpha_{3,i}(|x(t_k)|)\end{aligned}$$

from which we can obtain:

$$\begin{aligned}&\frac{\partial V_i(x(t))}{\partial x} f(x(t), u(t_k), w(t))\\ &\leq L'_{x,i}M\Delta + L'_{w,i}\theta - \alpha_{3,i}(\alpha_{2,i}^{-1}(\rho_{s,i}))\end{aligned} \tag{18a}$$

for $t \in [t_k, t_{k+1})$, where the last inequality follows from adding and subtracting $\frac{\partial V_i(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0)$ and using the triangle inequality, Eqs. 3b-3c, and $x(t_k) \in \Omega_{\rho_i}/\Omega_{\rho_{s,i}}$ with Eq. 2a. If Eq. 11 holds, then

$$\frac{\partial V_i(x(t))}{\partial x} f(x(t), u(t_k), w(t)) \leq -\epsilon_{w,i}/\Delta \tag{19}$$

Integrating Eq. 19 gives that $V_i(x(t)) \leq V_i(x(t_k))$, $\forall t \in [t_k, t_{k+1})$, such that if $x(t_k) \in \Omega_{\rho_i}/\Omega_{\rho_{s,i}}$, then $x(t) \in \Omega_{\rho_i}$, $\forall t \in [t_k, t_{k+1})$.

If instead $x(t_k) \in \Omega_{\rho_{s,i}} \subset \Omega_{\rho_i}$, then from Eq. 13, $x(t) \in \Omega_{\rho_{\min,i}} \subset \Omega_{\rho_i}$ for $t \in [t_k, t_{k+1})$. Therefore, if Eq. 5 is used to compute the input trajectory at t_k and $x(t_k) \in \Omega_{\rho_i}$ and Eq. 5g is applied, $x(t) \in \Omega_{\rho_i}$ for $t \in [t_k, t_{k+1})$ (regardless of whether Eq. 5f is applied). Because $\Omega_{\rho_i} \subseteq \Omega_{\rho_1}$, this indicates that when the LEMPC of Eq. 5 is used with Eq. 5g activated to determine the control action at t_k when $x(t_k) \in \Omega_{\rho_i}$, then $x(t) \in \Omega_{\rho_1}$ for $t \in [t_k, t_{k+1})$.

Finally, consider that $x(t_k) \in \Omega_{\rho_i}$ and $h_i(x(t_k))$ is used to control the process of Eq. 1 from t_k to t_{k+1} so that Eq. 2b holds at t_k. From similar steps as in Eq. 18 and if $x(t_k) \in \Omega_{\rho_i}/\Omega_{\rho_{s,i}}$ and Eq. 11 holds, then we can use similar steps as for Eq. 19 to derive that $V_i(x(t)) \leq V_i(x(t_k))$,

$\forall t \in [t_k, t_{k+1})$, such that if $x(t_k) \in \Omega_{\rho_i}/\Omega_{\rho_{s,i}}$, then $x(t) \in \Omega_{\rho_i}$, $\forall t \in [t_k, t_{k+1})$. If $x(t_k) \in \Omega_{\rho_{s,i}}$, then when Eq. 13 holds, we obtain that $x(t) \in \Omega_{\rho_{\min,i}}$, $t \in [t_k, t_{k+1})$, so that $x(t) \in \Omega_{\rho_i}$ for $t \in [t_k, t_{k+1})$. Since $\Omega_{\rho_i} \subseteq \Omega_{\rho_1}$, we obtain that if $x(t_k) \in \Omega_{\rho_i}$ and $h_i(x(t_k))$ is applied for $t \in [t_k, t_{k+1})$, then $x(t) \in \Omega_{\rho_1}$, $\forall\ t \in [t_k, t_{k+1})$. The above results indicate that the closed-loop state never leaves Ω_{ρ_1} in a sampling period if the conditions of Theorem 4 hold.

4. APPLICATION TO A CHEMICAL PROCESS EXAMPLE

To demonstrate the application of a set of LMPC's that are randomly selected at every t_k, we present a chemical process example involving a continuous stirred tank reactor (CSTR) in which the reaction $A \rightarrow B$ proceeds. The model parameters (feed and outlet volumetric flow rates F, feed temperature T_0, liquid density ρ_L, heat capacity C_p, liquid volume V, activation energy E, pre-exponential constant k_0, gas constant R_g, and enthalpy of reaction ΔH) are given in (Alanqar et al., 2015). The inputs are the feed concentration C_{A0} and heat rate Q added to or removed from the reactor, resulting in the model:

$$\dot{C}_A = \frac{F}{V}(C_{A0} - C_A) - k_0 e^{-\frac{E}{R_g T}} C_A^2 \tag{20a}$$

$$\dot{T} = \frac{F}{V}(T_0 - T) - \frac{\Delta H k_0}{\rho_L C_p} e^{-\frac{E}{R_g T}} C_A^2 + \frac{Q}{\rho_L C_p V} \tag{20b}$$

where C_A and T represent the concentration and temperature in the reactor. Deviation variable vectors for the states and inputs are as follows: $x = [x_1\ x_2]^T = [C_A - C_{As}\ T - T_s]^T$ and $u = [u_1\ u_2]^T = [C_{A0} - C_{A0s}\ Q - Q_s]^T$, where $C_{As} = 1.22\ \frac{kmol}{m^3}$, $T_s = 438.2\ K$, $C_{A0s} = 4\ \frac{kmol}{m^3}$, and $Q_s = 0\ \frac{kJ}{hr}$ are the steady-state values of C_A, T, C_{A0}, and Q at the operating steady-state. The control objective is to maximize the following economics-based stage cost for the process of Eq. 20 representing the production rate of B while computing control actions which meet the input constraints $0.5 \leq C_{A0} \leq 7.5\ \frac{kmol}{m^3}$ and $-5 \times 10^5 \leq Q \leq 5 \times 10^5\ \frac{kJ}{hr}$ and maintain closed-loop stability:

$$L_e = k_0 e^{-\frac{E}{R_g T}} C_A^2 \tag{21}$$

We first develop the set of LMPC's to be utilized to control the process of Eq. 20 in a manner that prevents a certain value of $x(t_k)$ from being as easily mapped to a specific input as it would be if a single LMPC were utilized throughout the time of operation. We begin by developing seven (i.e., $n_p = 7$) potential combinations of V_i, h_i, Ω_{ρ_i}, and $\Omega_{\rho_{e,i}}$. The form of each V_i is $x^T P_i x$, where P_i is a symmetric positive definite matrix of the following form:

$$\begin{bmatrix} P_{11} & P_{12} \\ P_{12} & P_{22} \end{bmatrix} \tag{22}$$

Sontag's control law (Lin and Sontag, 1991) was used to set the u_2 component of every $h_i = [h_{i,1}\ h_{i,2}]^T$ as follows:

$$h_{i,2}(x) = \begin{cases} -\dfrac{L_{\tilde{f}} V_i + \sqrt{L_{\tilde{f}} V_i^2 + L_{\tilde{g}_2} V_i^4}}{L_{\tilde{g}_2} V_i}, & \text{if } L_{\tilde{g}_2} V_i \neq 0 \\ 0, & \text{if } L_{\tilde{g}_2} V_i = 0 \end{cases} \tag{23}$$

where if $h_{i,2}$ fell below or exceeded the upper or lower bound on u_2, $h_{i,2}$ was saturated at the bound. In Eq. 23, $\tilde{f}$ represents the vector containing the terms in Eq. 20 (after it has been rewritten in deviation variable form in terms of x_1 and x_2) that do not contain any inputs, and $\tilde{g}$ represents the matrix that multiplies the vector of inputs u_1 and u_2 in this equation. $L_{\tilde{f}} V_i$ and $L_{\tilde{g}_k} V_i$ represent the Lie derivatives of V_i with respect to $\tilde{f}$ and $\tilde{g}_k$, $k = 1, 2$. For simplicity, $h_{i,1}$ was taken to be 0 $kmol/m^3$ for $i = 1, \ldots, 7$. Using the values of the entries of each P_i associated with each V_i in Table 1 and the associated h_i, $i = 1, \ldots, 7$, the stability regions in Table 1 were obtained. Subsets of these regions were selected to be $\Omega_{\rho_{e,i}}$ to allow a number of different control laws to be developed. The value of $\rho_{e,i}$ was not more than 80% of ρ_i in each case.

Table 1. $i-th$ controller parameters

i	P_{11}	P_{12}	P_{22}	ρ_i	$\rho_{e,i}$
1	1200	5	0.1	180	144
2	2000	-20	1	180	144
3	1500	-20	10	180	144
4	0.2	0	2000	180	144
5	1200	5	0.1	180	100
6	1200	5	0.1	180	130
7	1200	5	0.1	180	30

The process was initialized from $x_{init} = [-0.4\ kmol/m^3\ 20\ K]^T$ and was controlled under an LMPC with the form of Eq. 4 at all sampling times. We also initialized it from x_{init} but controlled it utilizing a randomized LMPC implementation strategy, where the implementation strategy in Section 3.2 was followed with the exception that δ was set to 0 at every sampling time, and only $h_1(x)$ was considered as a candidate controller at a given sampling time as an alternative to the controllers in Table 1. Therefore, at every sampling time, both the LMPC of Eq. 5 with $i = 1$ and $h_1(x)$ were allowable control actions, and the $i-th$ controller in Table 1 was also allowable if $x(t_k) \in \Omega_{\rho_i}$. The simulations were implemented in MATLAB R2016a by MathWorks® using fmincon and the seed rng(5) and random integer generation function randi when the randomized LMPC implementation strategy was used. The integration step for the model of Eq. 20 was set to $10^{-4}\ hr$, $N = 10$, and $\Delta = 0.01\ hr$, with 1 hr of operation utilized. The Lyapunov-based stability constraint activated when $x(t_k) \in \Omega_{\rho_{e,i}}$ was enforced at the end of every sampling period in the prediction horizon, and whenever the Lyapunov-based stability constraint involving the time-derivative of the Lyapunov function was enforced, the other Lyapunov-based constraint was implemented at the end of the sampling periods after the first.

Fig. 2 shows the state-space trajectories resulting from controlling the process with one LMPC throughout the time of operation, and Fig. 3 shows the results of controlling the LMPC with one of the eight potential control laws selected at every sampling time, but depending on the position of the state measurement in state-space. Both the single LMPC and the randomized LMPC implementation strategy were able to maintain the closed-loop state within Ω_{ρ_1}. The time-integral of Eq. 21 for the process of Eq. 20 was 32.2187 for the single LMPC and 27.7536 for the randomized LMPC implementation strategy. It is possible to consider an alternative implementation strategy in which the randomization only occurs at certain times (or potentially at random times) to seek to deter attackers but

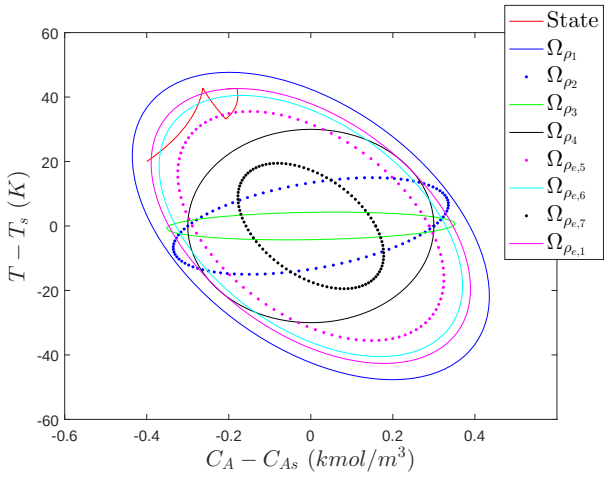

Fig. 2. State-space trajectories under the single LMPC for the CSTR of Eq. 20. The figure indicates that the closed-loop trajectory settled on the boundary of $\Omega_{\rho_{e,1}}$ to optimize L_e while meeting the constraints.

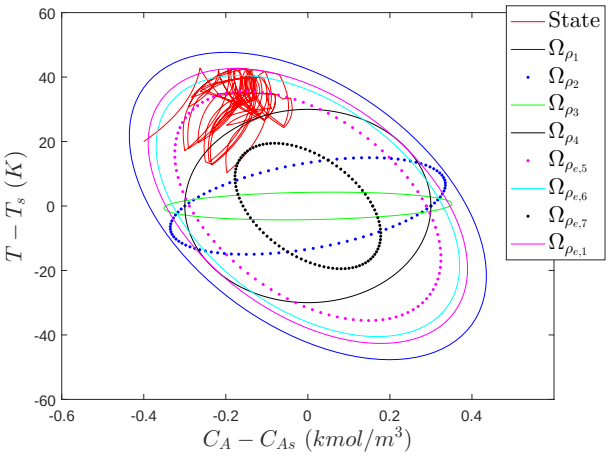

Fig. 3. State-space trajectories under the randomized LMPC implementation strategy for the CSTR of Eq. 20.

without requiring that the process always be operating in such a mode if it lowers profits. Despite the decrease in profits due to the randomization, both the single LMPC and the LMPC's implemented with the randomized implementation strategy outperformed steady-state operation, which had a value of the time-integral of Eq. 21 of 13.8847.

5. CONCLUSION

This work developed a randomized control implementation strategy with the goal of discouraging cyberattacks in which false state measurements are fed to an MPC. The implications of using the randomized control implementation strategy during normal operation (i.e., in the absence of a cyberattack) were studied. Future work will explore more deeply the properties of the control strategy in the presence of a cyberattack (e.g., design considerations for the randomized controllers which make the strategy create the most different potential input policies for the same measurement through the different controllers, conditions when the proposed strategy may be unfavorable, and alternative randomized control approaches for such situations).

REFERENCES

Alanqar, A., Ellis, M., and Christofides, P.D. (2015). Economic model predictive control of nonlinear process systems using empirical models. *AIChE Journal*, 61, 816–830.

Cárdenas, A.A., Amin, S., Lin, Z.S., Huang, Y.L., Huang, C.Y., and Sastry, S. (2011). Attacks against process control systems: Risk assessment, detection, and response. In *Proceedings of the ACM Asia Conference on Computer & Communications Security*. Hong Kong, China.

Chavez, A.R., Stout, W.M.S., and Peisert, S. (2015). Techniques for the dynamic randomization of network attributes. In *Proceedings of the IEEE International Carnahan Conference on Security Technology*, 1–6. Taipei, Taiwan.

Clark, R.M., Panguluri, S., Nelson, T.D., and Wyman, R.P. (2017). Protecting drinking water utilities from cyberthreats. *Journal - American Water Works Association*, 109, 50–58.

Heidarinejad, M., Liu, J., and Christofides, P.D. (2012). Economic model predictive control of nonlinear process systems using Lyapunov techniques. *AIChE Journal*, 58, 855–870.

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 49–51.

Lin, Y. and Sontag, E.D. (1991). A universal formula for stabilization with bounded controls. *Systems & Control Letters*, 16, 393–397.

Linda, O., Manic, M., and McQueen, M. (2013). Improving control system cyber-state awareness using known secure sensor measurements. In B.M. Hämmerli, N. Kalstad Svendsen, and J. Lopez (eds.), *Critical Information Infrastructures Security. CIRITIS 2012*, volume 17722 of *Lecture Notes in Computer Science*, 46–58. Springer, Berlin, Heidelberg.

Mhaskar, P., El-Farra, N.H., and Christofides, P.D. (2006). Stabilization of nonlinear systems with state and control constraints using Lyapunov-based predictive control. *Systems & Control Letters*, 55, 650–659.

Mhaskar, P., Liu, J., and Christofides, P.D. (2013). *Fault-Tolerant Process Control: Methods and Applications*. Springer-Verlag, London, England.

Muñoz de la Peña, D. and Christofides, P.D. (2008). Lyapunov-based model predictive control of nonlinear systems subject to data losses. *IEEE Transactions on Automatic Control*, 53, 2076–2089.

Perlroth, N. and Krauss, C. (2018). A cyberattack in Saudi Arabia had a deadly goal. Experts fear another try. `https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html`. Accessed: 2018-4-11.

Rosich, A., Voos, H., Li, Y., and Darouach, M. (2013). A model predictive approach for cyber-attack detection and mitigation in control systems. In *Proceedings of the IEEE Conference on Decision and Control*, 6621–6626. Florence, Italy.

Smith, R.E. (2013). *Elementary Information Security*. Jones & Bartlett Learning, LLC, Burlington, MA.