Actuator Cyberattack Handling Using Lyapunov-based Economic Model Predictive Control

Keshav Kasturi Rangan * **Henrique Oyama** * **Helen Durand** *

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

Abstract: Cybersecurity has gained increasing interest as a consequence of the potential impacts of cyberattacks on profits and safety. While attacks can affect various components of a plant, prior work from our group has focused on the impact of cyberattacks on control components such as process sensors and actuators and the development of detection strategies for cybersecurity derived from control theory. In this work, we provide greater focus on actuator attacks; specifically, we extend a detection and control strategy previously applied for sensor attacks and based on an optimization-based control technique called Lyapunov-based economic model predictive control (LEMPC) to detect attacks impacting the control action applied by the actuators when the state measurements provided to the controller are accurate. Closed-loop stability guarantees are rigorously derived. A continuous stirred tank reactor is simulated to elucidate aspects of the detection strategy proposed.

Keywords: Nonlinear processes, model predictive control, cybersecurity, nonlinear control, actuators

1 Introduction

Smart/next-generation manufacturing, which can lead to an increase in automation, enhanced safety, and greater operational efficiency, has received increasing attention in recent years. Due to its criticality, cybersecurity of control systems has been an active research area, with research covering topics ranging from control for linear systems in the presence of actuator or sensor attacks Fawzi et al. (2014) to using optimization to predict attack behavior Vamvoudakis et al. (2013). One of the topics that has received attention is active cyberattack detection schemes which attempt to force cyberattacks to become visible through changes to the system or operating policy. Examples of strategies in this category have included dynamic watermarking Satchidanandan and Kumar (2016), adjusting process dynamics Teixeira et al. (2012), or watermarking measurement and input signals Ghaderi et al. (2020).

This work uses a type of model predictive control (MPC) design called Lyapunov-based economic model predictive control (LEMPC) Heidarinejad et al. (2012), which is a formulation with strong closed-loop stability and feasibility properties in the presence of sufficiently small bounded disturbances and measurement noise. Other formulations that use LEMPC include machine learning detection strategies combined with LEMPC and implemented in both centralized Chen et al. (2020) and distributed Chen et al. (2021) fashions for maintaining closed-loop stability during normal process operation, with the possibility of maintaining closed-loop stability after an attack. Our group has analyzed cybersecurity for control systems from a nonlinear systems perspective Durand (2018). This led to the development of detection strategies for handling sensor measurement cyberattacks with safety guarantees for scenarios when process dynamics are constant Oyama and Durand (2020) as well as when they are changing over time Rangan et al. (2021); Oyama et al. (2021). While our recent work Oyama et al. (2022) addressed multiple detection strategies to handle simultaneous cyberattacks on both process sensors and actuators, this work did not provide a thorough discussion of attack detection for the case of actuator attacks only. Motivated by this gap, this work will provide details with an in-depth discussion of an LEMPC-based strategy for handling actuator attacks on nonlinear systems with guaranteed safety in the presence of undetected attacks.

2 Preliminaries

2.1 Notation

The Euclidean norm of a vector x is denoted by $|\cdot|$, and the transpose of x is denoted by x^T. A class $\mathcal{K}$ function $\alpha : [0, a) \to [0, \infty)$ is strictly increasing with $\alpha(0) = 0$. Set subtraction is signified by " / " such that $x \in A/B := \{x \in R^n : x \in A, x \notin B\}$. A level set of a positive definite function V is denoted by $\Omega_\rho := \{x \in R^n : V(x) \leq \rho\}$. $\mathbb{R}_+$ signifies the set of non-negative real numbers. A state measurement is available at every $t_k := k\Delta$, where $k = 0, 1, \ldots$, where Δ is the sampling period.

2.2 Class of Systems

This work addresses systems of the form:

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

where $x \in X \subset \mathbb{R}^n$, $u \in U \subset \mathbb{R}^m$, and $w \in W \subset \mathbb{R}^z$ are the state, input, and disturbance vectors, respectively, and f is locally Lipschitz on $X \times U \times W$, and $W := \{w \in \mathbb{R}^z : |w| \leq \theta_w, \theta_w > 0\}$. It is assumed that there exists a sufficiently smooth Lyapunov function $V : \mathbb{R}^n \to \mathbb{R}_+$, functions $\alpha_j(\cdot)$, $j = 1, \ldots, 4$, of class $\mathcal{K}$, and a controller $h(x) = [\bar{h}_1(x) \ \ldots \ \bar{h}_m(x)]^T$ capable of asymptotically stabilizing the closed-loop system to the origin of Eq. 1 in the absence of disturbances such that the following inequalities are satisfied:

$$\alpha_1(|x|) \leq V(x) \leq \alpha_2(|x|) \tag{2a}$$

$$\frac{\partial V(x)}{\partial x} f(x, h(x), 0) \leq -\alpha_3(|x|) \tag{2b}$$

$$\left|\frac{\partial V(x)}{\partial x}\right| \leq \alpha_4(|x|) \tag{2c}$$

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

$\forall x \in D \subset \mathbb{R}^n$ and D is an open neighborhood of the origin. $\Omega_\rho \subset D$ is considered to be the stability region of the nominal closed-loop system under the controller $h(x)$ where $x \in X$, $\forall x \in \Omega_\rho$. Furthermore, we consider that the components of $h(x)$ satisfy:

$$|\bar{h}_i(x) - \bar{h}_i(\hat{x})| \leq L_h |x - \hat{x}| \tag{3}$$

for all $x, \hat{x} \in \Omega_\rho$, $i = 1, \ldots, m$, and $L_h > 0$. The smoothness of V and local Lipschitz property of f give:

$$\begin{aligned} &|f(x_1, u_1, w) - f(x_2, u_2, 0)| \\ &\quad \leq L_x |x_1 - x_2| + L_u |u_1 - u_2| + L_w |w| \end{aligned} \tag{4a}$$

$$\begin{aligned} &\left|\frac{\partial V(x_1)}{\partial x} f(x_1, u, w) - \frac{\partial V(x_2)}{\partial x} f(x_2, u, 0)\right| \\ &\quad \leq L'_x |x_1 - x_2| + L'_w |w| \end{aligned} \tag{4b}$$

$$|f(x, u, w)| \leq M_f \tag{5}$$

$\forall x_1, x_2 \in \Omega_\rho$, $u, u_1, u_2 \in U$ and $w \in W$, where $L_x, L'_x, L_u, L_w, L'_w$, and M_f are positive constants.

2.3 Lyapunov-Based Economic Model Predictive Control (LEMPC)

In this work, we utilize an optimization-based control design known as LEMPC Heidarinejad et al. (2012), which is formulated as follows:

$$\min_{u(t) \in S(\Delta)} \quad \int_{t_k}^{t_{k+N}} L_e(\tilde{x}(\tau), u(\tau))\, d\tau \tag{6a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0) \tag{6b}$$

$$\tilde{x}(t_k) = x(t_k) \tag{6c}$$

$$\tilde{x}(t) \in X, \ \forall\, t \in [t_k, t_{k+N}) \tag{6d}$$

$$u(t) \in U, \ \forall\, t \in [t_k, t_{k+N}) \tag{6e}$$

$$\begin{aligned} &V(\tilde{x}(t)) \leq \rho_e, \ \ \forall\, t \in [t_k, t_{k+N}), \\ &\quad \text{if } x(t_k) \in \Omega_{\rho_e} \end{aligned} \tag{6f}$$

$$\begin{aligned} &\frac{\partial V(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0) \\ &\qquad \leq \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), h(x(t_k)), 0), \\ &\quad \text{if } x(t_k) \in \Omega_\rho / \Omega_{\rho_e} \end{aligned} \tag{6g}$$

where $u(t) \in S(\Delta)$ signifies that the optimal solution is a piecewise-constant input vector. N represents the length of the prediction horizon in terms of sampling periods, where each sampling period is of length Δ. The objective function is the time-integral of the economic stage cost L_e of Eq. 6a, evaluated throughout the prediction horizon. The predictions $\tilde{x}(t)$ are obtained from the nominal model of Eq. 6b. The state and input constraints are given by Eqs. 6d-6e respectively. The two Lyapunov-based stability constraints are given by Eqs. 6f and 6g.

3 Detecting and Handling Actuator Cyberattacks using LEMPC

Cyberattacks on control systems pose a threat due to their ability to directly manipulate physical systems resulting in effects ranging from reduced profits to loss of life. In our prior works Oyama and Durand (2020); Rangan et al. (2021), three strategies were developed to detect cyberattacks on sensor measurements. Oyama et al. (2022) extended these to handle attacks on actuators and on sensors and actuators at the same time. Because the focus of Oyama et al. (2022) was on this simultaneous actuator and sensor attack case, less attention was given to discussing handling of attacks on process actuators alone. In this manuscript, we provide further details on a detection strategy for the case that only actuators are attacked.

The strategy that will be analyzed in the subsequent sections is inspired by the first detection strategy presented in Oyama and Durand (2020) (developed for sensor measurement cyberattacks). In Oyama and Durand (2020), a detection strategy was developed that probes for attacks on sensors by modifying the control design in Eq. 6 at random times. Specifically, at random times, a new steady-state is selected around which the LEMPC of Eq. 6 is designed (creating new Lyapunov functions around this steady-state designated by V_i to reflect that they are designed with respect to the i-th steady-state), and then the constraint of Eq. 6g is enforced throughout the subsequent sampling period (without Eq. 6f being considered) to drive the closed-loop state toward that steady-state. The motivation for this is that when Eq. 6g is enforced, under sufficient conditions, the closed-loop state moves toward the i-th steady-state and V_i decreases over the sampling period. If it does not, an attack could be flagged.

When this strategy is extended to the case that actuators are attacked, we will no longer consider probing randomly, but instead will consider probing for attacks at every sampling time. In the absence of an attack, this will cause V_i to decrease, and the closed-loop state will be maintained within the stability region corresponding to the i-th steady-state. However, unlike in the sensor cyberattack case, the sensor measurements are now considered to be accurate; this means that if V_i does not actually decrease, an attack will be flagged. Though there is no guarantee that an attack cannot cause V_i to decrease (i.e., an attack may be "stealthy" in the sense that it evades the detection mechanism based on $\dot{V}_i$ being negative), a decrease in the value of V_i over a sampling period following the activation of the i-th LEMPC formulation under a rogue actuator signal sent to the process would still maintain the closed-loop state inside the i-th stability region under sufficient conditions. This discussion implies that the i-th LEMPC formulation detection strategy holds particular value for

handling actuator attacks when sensor measurements are not falsified. Specifically, though a major drawback of the detection strategy presented in Oyama and Durand (2020) for state measurement cyberattacks is that it did not guarantee safety when a falsified state measurement is provided to the i-th LEMPC (because even if the falsified state measurements decrease V_i, it does not imply that these false sensor measurements are translated by the controller into stabilizing control actions), safety is maintained in the presence of actuator attacks under this strategy. This is because the decrease in V_i (which is based on the state measurements) is "real" in the case of the actuator attack (since the state measurements are not falsified), resulting in the actual closed-loop state remaining within a characterizable region Ω_{ρ_i} (a level set of V_i around the i-th steady-state) of state-space over a sampling period when the attack is not detected. A consideration that must be made, however, is the impact that the constant probing for attacks could have on profits, since it causes the operating strategy to deviate from what would otherwise be observed. One idea for attempting to handle this would be to make use of an auxiliary LEMPC with the form of Eq. 6. This LEMPC could be used at the start of every sampling period to predict the economically-optimal state at the end of the current sampling period (in the absence of plant-model mismatch, and subject to the prediction horizon length). If this state is a steady-state for the process with the input in the input bounds (and meeting other sufficient conditions to be described below), it could be used as the i-th steady-state. Though this may sound attractive as a means for attempting to reduce profit loss while handling actuator cyberattacks, profit guarantees cannot be made in the presence of plant/model mismatch, and if the closed-loop state does not reach this i-th steady-state in a sampling period, the state prediction from the LEMPC of Eq. 6 will be different than it would have been if the i-th steady-state had been reached. The transient behavior over the sampling period also may not be the same during the probing as under the LEMPC of Eq. 6. This indicates that the use of the auxiliary LEMPC is unlikely to cause the profits during the probing to match those which would have been obtained without the cyberattack-probing.

3.1 Probing for Actuator Cyberattacks Using LEMPC: Formulation

The LEMPC formed around the i-th steady-state (referred to as the i-th LEMPC) has the following form:

$$\min_{u_i(t)\in S(\Delta)} \quad \int_{t_k}^{t_{k+N}} L_e(\tilde{x}_i(\tau), u_i(\tau))\, d\tau \tag{7a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}_i(t) = f_i(\tilde{x}_i(t), u_i(t), 0) \tag{7b}$$

$$\tilde{x}_i(t_k) = x_i(t_k) \tag{7c}$$

$$\tilde{x}_i(t) \in X_i,\ \forall\, t \in [t_k, t_{k+N}) \tag{7d}$$

$$u_i(t) \in U_i,\ \forall\, t \in [t_k, t_{k+N}) \tag{7e}$$

$$\frac{\partial V_i(\tilde{x}_i(t_k))}{\partial x} f_i(\tilde{x}_i(t_k), u_i(t_k), 0) \leq \frac{\partial V_i(\tilde{x}_i(t_k))}{\partial x}\, f_i(\tilde{x}_i(t_k), h_i(\tilde{x}_i(t_k)), 0) \tag{7f}$$

where $x_i(t_k)$ represents the state measurement in deviation variable form from the i-th steady-state, and f_i represents the right-hand side of Eq. 1 when it is written in deviation variable form from the i-th steady-state. u_i represents the input vector in deviation variable form from the steady-state input associated with the i-th steady-state. X_i and U_i represent the state and control constraint sets in deviation variable form from the i-th steady-state. When an actuator attack is performed, the control action computed by Eq. 7 is not the one which is actually applied to the process. Rather, it is replaced by a rouge control action.

3.2 Probing for Actuator Cyberattacks Using LEMPC: Implementation Strategy

The implementation strategy for the detection concept of Section 3.1 is described below (in the case that an attempt is made to use the auxiliary LEMPC of Eq. 6 to compute the i-th steady-state at every sampling time as described above):

(1) An auxiliary LEMPC ("A-LEMPC") with the form in Eq. 6 receives the state measurement $\tilde{x}(t_k)$ and is used to determine the steady-state to be used for the subsequent sampling period. Go to Step 2.
(2) Verify that the i-th steady-state determined in Step 1 satisfies several conditions: 1) The i-th region Ω_{ρ_i} must be a subset of the safe operating region Ω_ρ, designed to contain several level sets of V_i to be described in the following section; 2) The steady-state input required to maintain the closed-loop state at the i-th steady-state must be within the input bounds; 3) The state measurement $\tilde{x}(t_k)$ must be contained within Ω_{ρ_i} (specifically, it must be within a subset $\Omega_{\rho_i'}$ to be defined in the following section; and 4) $\tilde{x}(t_k)$ must not be in a neighborhood $\Omega_{\rho_{s,i}}$ of the i-th steady-state. If these requirements are not met for the steady-state determined in Step 1, select an alternative steady-state meeting these requirements. Go to Step 3.
(3) The control action computed by the i-th LEMPC of Eq. 7 for the sampling period from t_k to t_{k+1} is used to control the process according to Eq. 7. Go to Step 4.
(4) Evaluate the Lyapunov function value at the end of the sampling period. If V_i does not decrease between the beginning and end of a sampling period, flag a potential cyberattack and apply mitigating actions. Go to Step 5.
(5) ($t_k \leftarrow t_{k+1}$). Go to Step 1.

3.3 Probing for Actuator Cyberattacks Using LEMPC: Stability and Feasibility Analysis

For the time period until an actuator attack is detected, this section will prove recursive feasibility of the A-LEMPC and the i-th LEMPC's for the process of Eq. 1 under the implementation strategy of Section 3.2 in the presence of bounded process noise. Because the state measurements are assumed not to be impacted by the attacks, the sensor measurements are impacted only by noise, where the maximum bound on the norm of the difference between the measured state and the actual state is θ_v. The theorem below also provides a guarantee of safety of the process of Eq. 1 under the implementation strategy of Section 3.2 before an actuator cyberattack is detected (i.e., even if a stealthy attack is occurring). In

the following theorem, subscripts are added to some of the prior notation (e.g., the functions α_j, $j = 1, 2, 3, 4$, and h, or the constants M_f, L'_x, and L'_w) to indicate that the functions and parameters are considered for the model and Lyapunov functions corresponding to the i-th steady-state or a steady-state of the A-LEMPC.

Theorem 1. Consider the closed-loop system of Eq. 1 under the implementation strategy of Section 3.2 where no cyberattack is detected, and each control formulation, i.e., the A-LEMPC and the i-th LEMPC, use controllers $h_A(\cdot)$ and $h_i(\cdot)$, $i \geq 1$, respectively, that satisfy the inequalities in Eqs. 2a-2d and 3. Let $\epsilon_{W_i} > 0$, $\Delta > 0$, $N \geq 1$, $\Omega_{\rho_i} \subset \Omega_{\rho'_A} \subset \Omega_{\rho_A} \subset X_A$ for $i \geq 1$, $\rho_i > \rho'_i > \rho_{\min,i} > \rho_{s,i} > 0$, where $\Omega_{\rho'_i}$ is defined as a level set of Ω_{ρ_i} that guarantees that if $V_i(\tilde{x}_i(t_k)) \leq \rho'_i$, then $V_i(x_i(t_k)) \leq \rho_{samp,i}$, for $i = A$ or $i \geq 1$. Additionally, $\rho = \rho_A > \rho'_A > \rho_{e,A} > \rho_{\min,A} > \rho_{s,A} > 0$. Let the following inequalities be satisfied:

$$-\alpha_{3,i}(\alpha_{2,i}^{-1}(\rho_{s,i})) + L'_{x,i}M_{f,i}\Delta + L'_{x,i}\theta_v + L'_{w,i}\theta_w \leq -\epsilon'_{w,i}/\Delta,\ i = A, 1, 2, \ldots \tag{8}$$

$$\rho_{\min,i} = \max\{V_i(x_i(t)) : x_i(t_k) \in \Omega_{\rho_{s,i}}, t \in [t_k, t_{k+1}), w \in W\},\ i = A, 1, 2, \ldots \tag{9}$$

$$\epsilon'_{w,i} > \max_{\tilde{x}_i(t_k) \in \Omega_{\rho'_i}/\Omega_{\rho_{s,i}}} \Big| \min\{V_i(\tilde{x}_i(t_k)) : \tilde{x}_i(t_k) \in \Omega_{\rho'_i}/\Omega_{\rho_{s,i}} - \max\{V_i(\tilde{x}_i(t_{k+1})) : \tilde{x}_i(t_k) \in \Omega_{\rho'_i}/\Omega_{\rho_{s,i}},\ u_i \in U_i, w \in W,\ |x_i(t_p) - \tilde{x}_i(t_p)| \leq \theta_v,\ p = k, k+1\}\Big|, i = A, 1, 2, \ldots \tag{10}$$

$$\rho_{samp,i} = \max\{V_i(x_i(t_k)) : \tilde{x}_i(t_k) \in \Omega_{\rho'_i}, i = A, 1, 2, \ldots, |x_i(t_k) - \tilde{x}_i(t_k)| \leq \theta_v\} \tag{11}$$

$$\rho_{h,i} = \max\{V_i(\tilde{x}_i(t_{k+1})) : x_i(t_k) \in \Omega_{\rho_{samp,i}}, i = A, 1, 2, \ldots, u_i \in U_i, w \in W\} \tag{12}$$

$$\rho_i = \max\{V_i(x_i(t_{k+1})) : \tilde{x}_i(t_{k+1}) \in \Omega_{\rho_{h,i}}, |x_i(t_{k+1}) - \tilde{x}_i(t_{k+1})| \leq \theta_v\} \tag{13}$$

If $\tilde{x}_i(t_0) \in \Omega_{\rho'_i}/\Omega_{\rho_{s,i}}$, $x_i(t_0) \in \Omega_{\rho_i} \subset \Omega_{\rho'_A}$, $|\tilde{x}_i(t_0) - x_i(t_0)| \leq \theta_v$, and steady-states meeting the conditions in Step 2 of the implementation strategy are able to be found at every sampling time, then the closed-loop state and state measurement are maintained in Ω_{ρ_A} at all times before an attack is detected. Furthermore, if $\tilde{x}_i(t_k) \in \Omega_{\rho'_i}/\Omega_{\rho_{s,i}}$ and no attack occurs, V_i decreases along the measured state trajectory.

The proof consists of three parts. In the first part, recursive feasibility of both Eq. 6 and Eq. 7 at every sampling time under the implementation strategy is demonstrated. In the second part, we demonstrate that the state measurement remains within $\Omega_{\rho_i} \subset \Omega_{\rho_A}$ under the implementation strategy in Section 3.2 before an attack occurs or if an attack will not lead to detection at the next sampling time (allowing feasibility of the A-LEMPC and i-LEMPC's at each sampling time before an attack is detected), assuming that steady-states meeting the requirements in Step 2 of the implementation strategy can be located at every sampling time. We also demonstrate that V_i is decreasing for $t \in [t_k, t_{k+1})$ under the implementation strategy either in the absence of actuator attacks or in the presence of actuator attacks that do not lead to detection at the next sampling time. The third part of the proof demonstrates that if detection will occur at the next sampling time, then the closed-loop state and state measurement will still be within Ω_{ρ_A} at that time.

Part 1. At each sampling time, the A-LEMPC is solved followed by the i-th LEMPC. Feasibility of the A-LEMPC at every sampling time is guaranteed when the state measurement is within Ω_{ρ_A} (to be demonstrated in *Part 2*), with the feasible control action as h_A implemented in sample-and-hold throughout the prediction horizon. Specifically, $h_A(\tilde{x}_A(t_j))$, $j = k, \ldots, k+N-1$, for $t \in [t_j, t_{j+1})$, is a feasible solution to the A-LEMPC of Eq. 6 because it trivially satisfies Eq. 6g, satisfies Eq. 6d when $\Omega_{\rho_A} \subset X_A$, and satisfies Eq. 6e by Eq. 2d. Similarly, this control action satisfies Eq. 6f by the properties of the Lyapunov-based controller Muñoz de la Peña and Christofides (2008) where, if the conditions of Eqs. 8 and 9 are met, then if $\tilde{x}_A(t_j) \in \Omega_{\rho_A}/\Omega_{\rho_{s,A}}$, $V_A(\tilde{x}_A)$ decreases throughout the following sampling period (keeping the closed-loop state in Ω_{ρ_A}), or if $\tilde{x}_A(t_j) \in \Omega_{\rho_{s,A}}$, then $\tilde{x}_A(t) \in \Omega_{\rho_{\min,A}} \subset \Omega_{\rho_A}$ for $t \in [t_j, t_{j+1})$. By the same arguments, $h_i(\tilde{x}_i(t_j))$, $j = k, \ldots, k+N-1$, $t \in [t_j, t_{j+1})$, is a feasible solution to Eq. 7 at every sampling time.

Part 2. To demonstrate that the closed-loop state and state measurement are always maintained within $\Omega_{\rho_i} \subset \Omega_{\rho_A}$ under the conditions of the theorem until a sampling time where an attack is performed that will be detected at the subsequent sampling time, we begin by examining t_0. At t_0, from the statement of the theorem, $\tilde{x}_i(t_0) \in \Omega_{\rho'_i}$ (so that $x(t_0) \in \Omega_{\rho_{samp,i}} \subset \Omega_{\rho_A}$ from the implementation strategy and definition of $\Omega_{\rho'_i}$). Eqs. 7f and Eq. 2b give:

$$\frac{\partial V_i(\tilde{x}_i(t_0))}{\partial x} f_i(\tilde{x}_i(t_0), u_i(t_0), 0) \leq -\alpha_{3,i}(|\tilde{x}_i(t_0)|) \tag{14}$$

Furthermore, defining:

$$\dot{V}_i(x_i(\tau)) = \frac{\partial V_i(x_i(\tau))}{\partial x} f_i(x_i(\tau), u_i(t_0), w(\tau)) \tag{15}$$

for $\tau \in [t_0, t_1)$, and adding and subtracting $\frac{\partial V_i(\tilde{x}_i(t_0))}{\partial x} f_i(\tilde{x}_i(t_0), u_i(t_0), 0)$ from the right-hand side of Eq. 15, applying the triangle inequality, Eq. 14, Eq. 5, Eq. 2a and $\tilde{x}_i(t_0) \in \Omega'_{\rho_i}/\Omega_{\rho_{s,i}}$ gives:

$$\dot{V}_i(x_i(\tau)) \leq -\alpha_{3,i}(\alpha_{2,i}^{-1}(\rho_{s,i})) + L'_{x,i}M_{f,i}\Delta + L'_{x,i}\theta_v + L'_{w,i}\theta_w \tag{16}$$

for $\tau \in [t_0, t_1)$. When Eq. 8 holds, this indicates that the Lyapunov function value for the actual closed-loop state will be less at the end of the sampling period than at the beginning, and thus $x_i(t_1) \in \Omega_{\rho_{samp,i}} \subset \Omega_{\rho_A}$. However, because of measurement noise at the beginning and end of the sampling period, it does not guarantee that the measurement will decrease. This is ensured, however, if Eq. 10 holds, which enables the measured value of V_i to decrease between two sampling periods and therefore to be used in detecting whether an attack occurs. This also ensures that $\tilde{x}_i(t_1)$ is within $\Omega_{\rho'_i} \subset \Omega_{\rho_A}$.

Applying this recursively, it is demonstrated that when an attack will not be detected at the next sampling time, the closed-loop state measurement at the next sampling time will be within $\Omega_{\rho'_i}$ and the closed-loop state will be within $\Omega_{\rho_{samp,i}}$. Specifically, at t_1, a new steady-state will be generated. By the assumption of the theorem that it is possible to generate a new steady-state meeting the

requirements of Step 2 of the implementation strategy, $\tilde{x}_i(t_1) \in \Omega_{\rho_i'}/\Omega_{\rho_{s,i}}$ for the new value of i (and by the definition of $\Omega_{\rho_{samp,i}}$, $x_i(t_1) \in \Omega_{\rho_{samp,i}}$). The same arguments as were applied at t_0 then continue to hold so that the closed-loop state is maintained within $\Omega_{\rho_{samp,i}}$ throughout the next sampling period, while the next state measurement is in $\Omega_{\rho_i'}$. Finally, because the closed-loop state is maintained within each Ω_{ρ_i} before an attack that would be detected at the next sampling time occurs, it is also maintained in Ω_{ρ_A}, guaranteeing feasibility of the A-LEMPC at every sampling time before an attack is detected. Finally, without an attack detected at the next sampling time, V_i must decrease or else the attack would be detected.

Part 3. Because an attack can only be detected at the end of a sampling period using the method in Section 3.2 because it is based on evaluating whether V_i for the measurement at t_{k+1} decreased compared to its value for the measurement at t_k, it is possible that an attack is not detected over the sampling period before an increase in V_i is detected. Eqs. 11-13 ensure that the closed-loop state and measurement are within $\Omega_{\rho_i} \subset \Omega_{\rho_A'}$ when the attack is detected. Specifically, Eqs. 11-12 ensure that if the measurement at t_k is within $\Omega_{\rho_i'}$, then the state measurement is within $\Omega_{\rho_{samp,i}}$ so that the measurement by t_{k+1} could in a worst-case be within $\Omega_{\rho_{h,i}}$. Since this measurement can have noise, Eq. 13 dictates that the farthest that the actual closed-loop state could be at t_{k+1} when the measurement is within $\Omega_{\rho_{h,i}}$ is Ω_{ρ_i}, and thus the actual and measured states are within Ω_{ρ_A}.

3.4 Probing for Actuator Cyberattacks Using LEMPC: Chemical Process Example

In this section, we present a process example to illustrate the concepts described above, but without ensuring that control-theoretic conditions are met (i.e., the designs are not verified to be resilient to cyberattacks, but serve to demonstrate aspects of the implementation strategy apart from the theory). The example used is a continuous stirred tank reactor (CSTR) in which a second-order, irreversible, exothermic reaction $A \rightarrow B$ occurs. The dynamics of the CSTR are as follows:

$$\dot{C}_A = \frac{F}{V}(C_{A0} - C_A) - k_0 e^{-\frac{E}{R_g T}} C_A^2 \tag{17}$$

$$\dot{T} = \frac{F}{V}(T_0 - T) - \frac{\Delta H k_0}{\rho_L C_p} e^{-\frac{E}{R_g T}} C_A^2 + \frac{Q}{\rho_L C_p V} \tag{18}$$

Here, the state of the system is given by the reactant concentration of species A, C_A and temperature in the reactor, T. The manipulated inputs are the reactant feed concentration of species A, C_{A0}, and the heat rate Q. The values of the parameters used in the simulation are $V = 1m^3$, $T_0 = 300K$, $C_p = 0.231kJ/kg \cdot K$, $k_0 = 8.46 \times 10^6 m^3/\text{h}\cdot\text{kmol,F} = 5\text{m}^3/h$, $\rho_L = 1000kg/m^3$, $E = 5 \times 10^4 kJ/kmol$, $R_g = 8.314kJ/kmol \cdot K$, $\Delta H = -1.15 \times 10^4 kJ/kmol$. The vectors of the state and input of the process in deviation variable form are given by, $x_1 = [x_{1,1}\ x_{1,2}]^T = [C_A - C_{As}\ T - T_s]^T$ and $u_1 = [u_{1,1}\ u_{1,2}]^T = [C_{A0} - C_{A0s}\ Q - Q_s]^T$ where the steady-state values are $x_{1s} = [C_{As}\ T_s]^T = [1.22\,\text{kmol/m}^3\ 438.2\,\text{K}]^T$, $[C_{A0s}\ Q_s]^T = [4.0\,\text{kmol/m}^3\ 0\,\text{kJ/h}]^T$. The Explicit Euler method is used to numerically integrate the process model, Eqs. 17-18, by using an integration step of 10^{-4} h. The economic cost function is selected to be $L_e = k_0 e^{-E/(RT)} C_A^2$.

We first demonstrate the concept that attacks can be undetected while decreasing the Lyapunov function when a constraint inspired by that in Eq. 7f is used. We consider a case with no noise or disturbances (i.e., no plant/model mismatch). For these simulations, Ω_{ρ_1} was developed using the Lyapunov function $V_1 = x_1^T P x_1$, where $P = [1200\ 5; 5\ 0.1]$, the Lyapunov-based controller $h_1(x_1) = [\bar{h}_{1,1}(x_1)\ \bar{h}_{1,2}(x_1)]^T$ with components $\bar{h}_{1,1}(x_1)$ set to 0 kmol/m^3 and $\bar{h}_{1,2}(x_1)$ designed via Sontag's control law Lin and Sontag (1991), $\rho_1 = 300$, and $\rho_{e,1} = 225$. A second stability region Ω_{ρ_2} was also developed that is contained within Ω_{ρ_1}. A variety of methods could be used to obtain an alternative steady-state; here, no attempt was made to optimize economics, and a random alternative steady-state $x_{2s} = [1.22\,\text{kmol/m}^3\ 450\,\text{K}]^T$ was selected for the design of Ω_{ρ_2}, where $V_2(x) = x_2^T P_2 x_2$, with $x_2 = x_1 + x_{1s} - x_{2s}$, $P_2 = [2100\ 10; 10\ 0.25]$, and $\rho_2 = 100$. The i-th LEMPC design using Ω_{ρ_2} was designed using a Lyapunov-based controller with components $h_{2,1}(x_2) = 0$ kmol/m^3 and $h_{2,2}(x_2)$ selected using Sontag's control law with respect to $V_2(x_2)$. In each LEMPC, $N = 10$ and $\Delta = 0.01$ h, and the value of the decision variable corresponding to Q was scaled down by 10^5. The LEMPC optimization problems were solved in MATLAB using fmincon.

The process was initialized at the state $x_{1,init} = [x_{1,1}(t_0)\ x_{1,2}(t_0)]^T = [-0.21\,\text{kmol/m}^3\ 28.89\,\text{K}]^T$ (in deviation variable form from x_{1s}) and simulated over 0.1 h of operation under four different cases: 1) at t_0, the LEMPC used for probing was designed using the $i = 1$ steady-state and Ω_{ρ_1} (i.e., the LEMPC of Eq. 7 was used with $i = 1$ and implemented by enforcing Eq. 7f at the end of the first sampling period), but the falsified input applied to the process in place of the LEMPC's input was a constant actuator output of $u_{1,1} = 0$ kmol/m^3 and $u_{1,2} = 0$ kJ/h ("Attack 1"); 2) at t_0, the LEMPC used for probing was designed using the $i = 2$ steady-state and Ω_{ρ_2} with the falsified input of Attack 1; 3) at t_0, the LEMPC used for probing was designed using the $i = 1$ steady-state and Ω_{ρ_1}, but the falsified input applied to the process in place of the LEMPC's input was a constant actuator output of $u_{1,1} = 1.657$ kmol/m^3 and $u_{1,2} = -1.141 \times 10^5$ kJ/h ("Attack 2"); and 4) at t_0, the LEMPC used for probing was designed using the $i = 2$ steady-state and Ω_{ρ_2} with the falsified input of Attack 2. It can be observed in Fig. 1 that under Attack 1, whether the value of V_1 or V_2 is evaluated over time, the attack would be flagged as the Lyapunov function increases over the subsequent sampling period. However, Attack 2 would not be detected by either of the two LEMPC formulations in that sampling period.

We now consider attempting to use a control law in the spirit of LEMPC for developing the steady-state to track (instead of random steady-state selection). In this case, the closed-loop system is again initialized from $x_{1,init}$, but a controller with a form inspired by Eq. 6 with $\tilde{x}(t_k)$ set to $x_{1,init}$ is solved. The first control action is then used to simulate the closed-loop system in open-loop to investigate whether the state prediction at t_{k+1} would serve as a suitable x_{2s}. Even for this case where the control

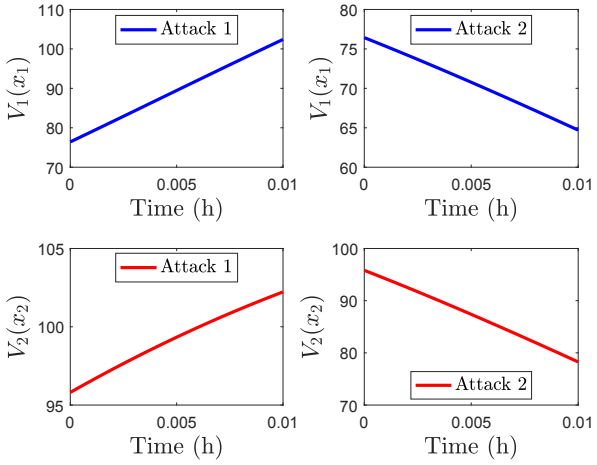

Fig. 1. V_1 (top plots) and V_2 (bottom plots) profiles over 0.1 h of operation for the process example in the presence of different actuator cyberattack policies, with no plant/model mismatch.

theory is not rigorously met, it would be required that for driving the closed-loop state to a neighborhood of a steady-state, that steady-state must be able to be reached with inputs within the input bounds. In this case, however, the predicted state after a single sampling period is at $C_A = 1.016$ kmol/m^3 and $T = 491.52$ K, which would require an input outside of the input bounds to maintain the closed-loop state at this condition. Therefore, though the closed-loop state prediction might pass through this condition, it would not be able to remain at it. Various strategies might be considered at this point for selecting a new steady-state, such as exploring whether there are steady-states within a ball around the predicted state from the LEMPC that have the largest steady-state profit while meeting the input constraints. However, as noted above, it would be challenging in general to make profit guarantees.

4 Conclusion

This work discusses an actuator cyberattack-handling procedure for next-generation manufacturing systems in the context of economic model predictive control. Using a Lyapunov-based formulation of this control framework with guarantees on the decrease of the Lyapunov function over a sampling period following activation of a constraint in the controller, we developed a strategy for detecting actuator attacks. The reformulation of the controller is performed in a manner that guarantees feasibility of both an auxiliary and reformulated LEMPC's at every sampling time, and also maintains the closed-loop state and state measurement within a characterizable region at all times when an attack is not detected (even in the presence of bounded measurement noise).

Acknowledgements

Financial support from the National Science Foundation CNS-1932026 and Wayne State University is gratefully acknowledged.

Literature Cited

Chen, S., Wu, Z., and Christofides, P.D. (2020). A cyber-secure control-detector architecture for nonlinear processes. *AIChE Journal*, 66(5), e16907.

Chen, S., Wu, Z., and Christofides, P.D. (2021). Cybersecurity of centralized, decentralized, and distributed control-detector architectures for nonlinear processes. *Chemical Engineering Research and Design*, 165, 25–39.

Durand, H. (2018). A nonlinear systems framework for cyberattack prevention for chemical process control systems. *Mathematics*, 6(9), 169.

Fawzi, H., Tabuada, P., and Diggavi, S. (2014). Secure estimation and control for cyber-physical systems under adversarial attacks. *IEEE Transactions on Automatic control*, 59(6), 1454–1467.

Ghaderi, M., Gheitasi, K., and Lucia, W. (2020). A blended active detection strategy for false data injection attacks in cyber-physical systems. *IEEE Transactions on Control of Network Systems*, 8(1), 168–176.

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.

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

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(9), 2076–2089.

Oyama, H. and Durand, H. (2020). Integrated cyberattack detection and resilient control strategies using Lyapunov-based economic model predictive control. *AIChE Journal*, 66(12), e17084.

Oyama, H., Messina, D., Rangan, K.K., and Durand, H. (2022). Lyapunov-based economic model predictive control for detecting and handling actuator and simultaneous sensor/actuator cyberattacks on process control systems. *Frontiers in Chemical Engineering*, 4, 810129.

Oyama, H., Rangan, K.K., and Durand, H. (2021). Handling of stealthy sensor and actuator cyberattacks on evolving nonlinear process systems. *Journal of Advanced Manufacturing and Processing*, 3(3), e10099.

Rangan, K.K., Oyama, H., and Durand, H. (2021). Integrated cyberattack detection and handling for nonlinear systems with evolving process dynamics under Lyapunov-based economic model predictive control. *Chemical Engineering Research and Design*, 170, 147–179.

Satchidanandan, B. and Kumar, P.R. (2016). Dynamic watermarking: Active defense of networked cyber–physical systems. *Proceedings of the IEEE*, 105(2), 219–240.

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. IEEE.

Vamvoudakis, K.G., Hespanha, J.P., Kemmerer, R.A., and Vigna, G. (2013). Formulating cyber-security as convex optimization problems. In *Control of Cyber-Physical Systems*, 85–100. Springer.