10-5-2020

Integrated Cyberattack Detection and Resilient Control Strategies using Lyapunov-Based Economic Model Predictive Control

Henrique Oyama
Wayne State University, gq6229@wayne.edu

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

Recommended Citation

Oyama, H. and Durand, H. (2020), Integrated Cyberattack Detection and Resilient Control Strategies using Lyapunov-Based Economic Model Predictive Control. AIChE J. doi: 10.1002/aic.17084

Integrated Cyberattack Detection and Resilient Control Strategies using Lyapunov-Based Economic Model Predictive Control

Henrique Oyama[a], Helen Durand[*,a]

[a] *Department of Chemical Engineering and Materials Science, Wayne State University, Detroit, MI 48202, USA.*

Abstract

The use of an integrated system framework, characterized by numerous cyber/physical components (sensor measurements, signals to actuators) connected through wired/wireless networks, has not only increased the ability to control industrial systems, but also the vulnerabilities to cyberattacks. State measurement cyberattacks could pose threats to process control systems since feedback control may be lost if the attack policy is not thwarted. Motivated by this, we propose three detection concepts based on Lyapunov-based economic model predictive control (LEMPC) for nonlinear systems. The first approach utilizes randomized modifications to an LEMPC formulation online to potentially detect cyberattacks. The second method detects attacks when a threshold on the difference between state measurements and state predictions is exceeded. Finally, the third strategy utilizes redundant state estimators to flag deviations from "normal" process behavior as cyberattacks.

Key words: Control system cybersecurity, model predictive control, chemical process control, nonlinear systems, state estimation.

Introduction

The chemical process industries are potential targets for cyberattacks, with motivations for such attacks ranging from sabotage of equipment to intellectual property theft.[1,2] Attacks on elements of control systems have the potential to create unsafe or economically unfavorable operating conditions. In light of this, attack detection has received focus in the literature (e.g.,[3,4]). Attack detection methods for cyber-physical systems have included those which are data-based for applications such as water systems[5] and smart grids.[6] In addition, resilient control designs based on state estimation

[*] Corresponding author: H. Durand, Tel: +1 (313) 577-3475; E-mail: helen.durand@wayne.edu.

have been developed for handling and detecting attacks. For example, Cardenas *et al.*[4] proposes cyberattack-resilient control frameworks that compare state estimates based on representative models of the physical system and (potentially corrupted) state measurements to detect an attack. In,[7] the theoretical conditions for a linear system that bound the maximum number of sensors that may provide false measurements while still allowing reconstruction of the state for a feedback controller are defined.

The incorporation of cyberattack detection and resilience into control systems also has been studied in the context of model predictive control (MPC[8]), an advanced control methodology that uses optimization to determine the inputs to a plant. In the power systems domain, MPC has been integrated with data-based detection and state reconstruction via a process model to recover performance of the power grid in the presence of sensor attacks.[9] For linear systems, MPC designs have been explored that can guarantee exponential stability of the origin in the presence of sufficiently short denial of service attacks,[10] guarantee boundedness of the closed-loop state in an invariant set under random cyberattacks on the sensor measurements,[11] and handle replay attacks.[12] For nonlinear systems, Chen *et al.*[13] combined a neural network-based attack detection technique developed in[3] with a two-layer control architecture, where the upper layer is a Lyapunov-based MPC, to guarantee closed-loop stability after attacks are detected. Durand[14] explored several MPC techniques with economics-based objective functions (known as economic MPC's (EMPC's)[15,16]) in the presence of false sensor measurements to explore cyberattacks in a nonlinear systems context. The impacts of cyberattacks on MPC's were also related to process and equipment design in.[17] However, further understanding of the interaction between cyberattack detection strategies and MPC/EMPC formulation and stability guarantees is still needed.

This motivates our development in this work of three cyberattack detection strategies that are integrated with a specific control framework known as Lyapunov-based EMPC (LEMPC),[18] enabling the co-design of the control and detection frameworks to provide guarantees regarding detection characteristics and closed-loop stability in the absence of and, under sufficient conditions and potentially for limited timeframes, the presence of, cyberattacks. The first control/detection strategy toggles between a full state feedback LEMPC and variations on that control law that are randomly generated over time to probe for cyberattacks. The second control/detection strategy also utilizes full state feedback LEMPC, but the detection is based on the state prediction from the prior state measurement to identify an attack while maintaining the closed-loop state within a characterizable region over one sampling period after an attack that is not detected. Finally the third control/detection concept is developed using output feedback LEMPC and comparing multiple redundant state estimates based on the available state measurements to signal an attack when the estimates do not agree while ensuring closed-loop stability under sufficient conditions (which include that not all sensors can be attacked). This work extends the results presented in.[19,20] The attack type considered throughout is a sensor measurement cyberattack due to the consistency of this attack with the attack design considered in various other works (e.g.,[4]) and due to the primary goal of this paper being an exploration of what might be possible to achieve with integrated control/detection strategies utilizing LEMPC for nonlinear systems.

Preliminaries

Notation

The notation $|\cdot|$ signifies the Euclidean norm of a vector. $\alpha : [0, a) \to [0, \infty)$ is a class $\mathcal{K}$ function if $\alpha(0) = 0$ and the function is continuous and strictly increasing. Ω_ρ denotes a level set of a scalar-valued function V (i.e., $\Omega_\rho := \{x \in R^n \ : \ V(x) \le \rho\}$). Set subtraction is signified by $'/'$ (i.e., $A/B := \{x \in R^n \ : \ x \in A, \ x \notin B\}$). x^T is the transpose of the vector x. A sampling time is denoted by $t_k := k\Delta$, $k = 0, 1, \ldots$, where Δ is a sampling period.

Class of Systems

This work considers the following class of systems:

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

where $x \in X \subset R^n$, $u \in U \subset R^m$, and $w \in W \subset R^z$ are the state, input, and disturbance vectors, respectively, and f is locally Lipschitz on $X \times U \times W$. We define $W := \{w \in R^z \mid |w| \le \theta_w, \ \theta_w > 0\}$ and $U := \{u \in R^m | \ |u| \le u^{\max}\}$. We consider that the "nominal" system of Eq. 1 ($w \equiv 0$) is stabilizable such that there exists an asymptotically stabilizing feedback control law $h(x)$, a sufficiently smooth Lyapunov function V, and class $\mathcal{K}$ functions $\alpha_i(\cdot)$, $i = 1, 2, 3, 4$, where:

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

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

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

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

$\forall\ x \in D \subset R^n$ (D is an open neighborhood of the origin). We define $\Omega_\rho \subset D$ to be the stability region of the nominal closed-loop system under the controller $h(x)$ and require that it be chosen such that $x \in X$, $\forall x \in \Omega_\rho$. Furthermore, we consider that $h(x)$ satisfies:

$$|h_i(x) - h_i(\hat{x})| \leq L_h|x - \hat{x}| \tag{3}$$

for all $x, \hat{x} \in \Omega_\rho$, with $L_h > 0$, where h_i is the i-th component of h, $i = 1, \dots, m$.

Because V is a sufficiently smooth function and f is locally Lipschitz, the following hold:

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

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

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

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

Observability assumption

We consider that there are M sets of measurements $y_i \in R^{q_i}$, $i = 1, \dots, M$, available at t_k:

$$y_i(t) = k_i(x(t)) + v_i(t) \tag{6}$$

where k_i is a vector-valued function, and v_i represents the measurement noise associated with the measurement y_i. We assume that the measurement noise is bounded (i.e., $v_i \in V_i := \{v_i \in R^{q_i} \mid |v_i| \leq \theta_{v,i},\ \theta_{v,i} > 0$) and that measurements of each y_i are continuously available. It is considered that for each of the M sets of measurements, a deterministic observer exists defined as:

$$\dot{z}_i = F_i(\epsilon_i, z_i, y_i) \tag{7}$$

where z_i is the estimate of the process state from the i-th observer, $i = 1, \ldots, M$, F_i is a vector-valued function, and $\epsilon_i > 0$. When a controller $h(z_i)$ with Eq. 7 is used to control the closed-loop system of Eq. 1, we make the following assumptions.

Assumption 1. [21, 22] *There exist positive constants* θ_w^*, $\theta_{v,i}^*$, *such that for each pair* $\{\theta_w, \theta_{v,i}\}$ *with* $\theta_w \leq \theta_w^*$, $\theta_{v,i} \leq \theta_{v,i}^*$, *there exist* $0 < \rho_{1,i} < \rho$, $e_{m0i} > 0$ *and* $\epsilon_{Li}^* > 0$, $\epsilon_{Ui}^* > 0$ *such that if* $x(0) \in \Omega_{\rho_{1,i}}$, $|z_i(0) - x(0)| \leq e_{m0i}$ *and* $\epsilon_i \in (\epsilon_{Li}^*, \epsilon_{Ui}^*)$, *the trajectories of the closed-loop system are bounded in* Ω_ρ, $\forall\ t \geq 0$.

Assumption 2. [21, 22] *There exists* $e_{mi}^* > 0$ *such that for each* $e_{mi} \geq e_{mi}^*$, *there exist* $t_{bi}(\epsilon_i)$ *such that* $|z_i(t) - x(t)| \leq e_{mi}$, $\forall\ t \geq t_{bi}(\epsilon_i)$.

Remark 1. High-gain observers,[23] which are typically analyzed for input-affine systems with a specific structure (a sub-class of the class of systems of Eq. 1), can satisfy Assumptions 1-2 for that class of input-affine systems under sufficient conditions.

Lyapunov-based Economic Model Predictive Control

LEMPC[18] is defined by the optimization problem:

$$\min_{u(t) \in S(\Delta)} \int_{t_k}^{t_{k+N}} L_e(\tilde{x}(\tau), u(\tau))\, d\tau \tag{8a}$$

$$\text{s.t.}\quad \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0) \tag{8b}$$

$$\tilde{x}(t_k) = x(t_k) \tag{8c}$$

$$\tilde{x}(t) \in X, \forall\, t \in [t_k, t_{k+N}) \tag{8d}$$

$$u(t) \in U,\ \forall\, t \in [t_k, t_{k+N}) \tag{8e}$$

$$V(\tilde{x}(t)) \leq \rho_{e,1},\ \text{if } x(t_k)\ \in\ \Omega_{\rho_{e,1}} \tag{8f}$$

$$\frac{\partial V(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0) \leq \frac{\partial V(x(t_k))}{\partial x}\ f(x(t_k), h(x(t_k)), 0),\ \text{if}\ \ x(t_k) \in \Omega_\rho / \Omega_{\rho_{e,1}} \tag{8g}$$

where the notation $u(t) \in S(\Delta)$ denotes that $u(t)$ is a piecewise-constant input vector with N pieces (N is the prediction horizon), each held for a sampling period of length Δ. The time integral of the stage cost L_e in Eq. 8 is evaluated from t_k to t_{k+N} with predictions $\tilde{x}$ of the process state obtained from Eq. 8b (which represents the "nominal" model, i.e., the model of Eq. 1 with $w(t) \equiv 0$). Eq. 8b is initialized from the measured state $x(t_k)$ at t_k via Eq. 8c. Eqs. 8d-8e represent state and input constraints, respectively. LEMPC is applied in a receding horizon fashion, with the optimal input computed for $t \in [t_k, t_{k+1})$ implemented in a sample-and-hold fashion. $\Omega_{\rho_{e,1}} \subset \Omega_\rho$ is a level set of V which renders Ω_ρ forward invariant under the LEMPC of Eq. 8.

Combining Cyberattack Detection and Process Control

In this section, we will develop several techniques for detecting and handling cyberattacks on controllers that have a form like that in Eq. 8. In a prior work by Wu et al.[3] that considered cyberattack detection mechanisms for nonlinear systems in tandem with a variation on LEMPC, a neural network-based detection method was designed to detect specific cyberattack scenarios (e.g., a min-max cyberattack, in which the minimum or maximum allowable sensor measurement values are provided to the control system), and the controller was assumed to use the state measurement from secure/redundant sensors after an attack was detected to attempt to maintain the closed-loop state in a bounded region of state-space. The data-based detection and control method from[3] may achieve appropriate performance for a cyberattack event, but does not guarantee that a cyberattack will be detected. The present manuscript utilizes a control-theoretic, rather than data-based, framework to develop three cyberattack detection methods. A goal of this is to avoid the potential limitation of data-driven methods that they may lack guarantees on detection. The first control/detection strategy uses a full state feedback LEMPC as the primary process controller and randomly develops other LEMPC formulations with the contractive constraint of Eq. 8g always activated that are used in place of the primary controller for short periods of time to potentially detect if an attack is happening. The second control/detection strategy also uses full state feedback LEMPC, but the detection method is based on the state prediction from the last state measurement and it maintains the closed-loop state within the stability region over one sampling period after the attack under sufficient conditions. Finally, the third control/detection concept uses output feedback LEMPC and state estimates based on the available state measurements to identify an attack while guaranteeing that the closed-loop state will not leave the stability region under sufficient conditions.

Detection Strategy 1: Randomized LEMPC Changes to Probe for Cyberattacks

In this section, a potential methodology for probing for cyberattacks is proposed that uses random modifications of the control design in Eq. 8 in a way that should create an expected outcome if no attack is occurring. Specifically, in the absence of an attack, if the contractive constraint of Eq. 8g is activated, the time derivative of the Lyapunov function along the closed-loop state trajectory under the controller $h(x)$ is expected to be negative (this would only potentially not occur if the closed-loop state was in a neighborhood of the steady-state), and therefore, when Eq. 8g is activated, it would be expected that the Lyapunov function (evaluated at the state measurements) should decrease for $t \in [t_k, t_{k+1}]$. If this did not occur, the process behavior could be considered abnormal, and could be flagged as potentially reflecting a cyberattack. However, a stealthy attacker who knows the LEMPC control law might try to provide state measurements that imply that the Lyapunov function decreases over the subsequent sampling period when that should occur according to the formulation in Eq. 8, but cause rogue control actions to be computed. To attempt to prevent this, we can consider randomly developing new control laws (here selected as LEMPC's) with characterizable behavior in the absence of an attack (here, a decrease in the value of the Lyapunov function for the randomly developed LEMPC for $t \in [t_k, t_{k+1}]$), and employ them at random times to make it harder for an attacker to provide false state measurements that would evade probing for attacks.

We refer to the LEMPC design around the operating steady-state as the (baseline) 1-LEMPC, which has stability region Ω_{ρ_1}, stability region subset $\Omega_{\rho'_{e,1}}$, Lyapunov function V_1, and controller h_1 used in its design. The alternative LEMPC's will be referred to as j-LEMPC designs (for $j > 1$) with stability region Ω_{ρ_j}, Lyapunov function V_j, and controller h_j used in the control design, and developed around steady-states that are potentially different from the operating steady-state (the j-th steady-states). We also define f_j as the model of Eq. 1 rewritten to have its origin at the j-th steady-state, and x_j and u_j as x and u in deviation variable form from the j-th steady-state (X_j and U_j represent the state and input sets in deviation form from the j-th steady-state). Furthermore, we assume that V_j and h_j satisfy Eqs. 2-5 with $\alpha_p(\cdot)$, $p = 1, 2, 3, 4$, U, L_x, L_w, L'_x, L'_w, L_u, L_x, L_h and M_f replaced by $\alpha_{p,j}(\cdot)$, $p = 1, 2, 3, 4$, U_j, $L_{x,j}$, $L_{w,j}$, $L'_{x,j}$, $L'_{w,j}$, $L_{u,j}$, $L_{x,j}$, $L_{h,j}$ and $M_{f,j}$.

The implementation strategy for cyberattack probing uses random generation of steady-states with stability regions contained within Ω_{ρ_1} of the (baseline) 1-LEMPC and that have steady-state inputs within U to develop new j-LEMPC ($j > 1$) designs online which can drive the closed-loop state toward the new (j-th) steady-state in the absence of a cyberattack. The LEMPC of Eq. 8 (with full state feedback) is used until a random sampling time $t_{s,j}$, $j = 2, 3\ldots$, when $x(t_k) \in \Omega_{\rho_1}$, at which time it is desired to run a check to determine whether a cyberattack is occurring. At this random time, a (j-th) steady-state is selected that has a stability region around it (Ω_{ρ_j}, $j > 1$), contained within Ω_{ρ_1}, that includes $x(t_k)$ (to ensure that V_j can be decreased in the absence of an attack from t_k to t_{k+N} if an LEMPC with Eq. 8g is used, which can only be guaranteed if the initial condition is within the stability region for the j-LEMPC, while being maintained within Ω_{ρ_1} so that closed-loop stability within Ω_{ρ_1} can be maintained when the j-th LEMPC switches back to the 1-LEMPC after probing). Furthermore, it must be ensured that the designed stability region does not have $x(t_k)$ within a neighborhood of the origin of the new stability region within which V_j would not be guaranteed to decrease due to the sample-and-hold controller implementation and disturbances. Once a suitable stability region is generated at $t_{s,j}$ meeting these requirements, an LEMPC of the form of Eq. 8, but formulated with respect to the j-th steady-state and with Eq. 8g always activated regardless of the position of the initial state, is selected to control the system for the next sampling period. Under the sufficient conditions to be developed in Section "Randomized LEMPC Changes to Probe for Cyberattacks: Stability and Feasibility Analysis," this ensures a decrease of V_j over the sampling period following $t_{s,j}$. Then, at $t_{e,j}$, the j-LEMPC switches back to operation under the (baseline) 1-LEMPC. The false state measurement cyberattacks in this section are assumed to lie within Ω_{ρ_1} to prevent detection on the basis of the state measurement being outside of the stability region that it should not exit.

Randomized LEMPC Changes to Probe for Cyberattacks: Formulation

The following two LEMPC formulations are proposed to probe for cyberttacks by interchanging between these LEMPC designs at random times. These have a form like that in Eq. 8, but one does not have the constraint of Eq. 8f, and both have different steady-states and Lyapunov-based constraint designs compared to one another. The baseline LEMPC is formulated as follows, which is used if $t_{e,j-1} \leq t < t_{s,j}$, $j = 2, \ldots$, where $t_{e,1} = 0$:

$$\min_{u_1(t) \in S(\Delta)} \int_{t_k}^{t_{k+N}} L_e(\tilde{x}_1(\tau), u_1(\tau))\, d\tau \tag{9a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}_1(t) = f_1(\tilde{x}_1(t), u_1(t), 0) \tag{9b}$$

$$\tilde{x}_1(t_k) = \tilde{x}_{b,1}(t_k) \tag{9c}$$

$$\tilde{x}_1(t) \in X_1,\ \forall\, t \in [t_k, t_{k+N}) \tag{9d}$$

$$u_1(t) \in U_1,\ \ \forall\, t \in [t_k, t_{k+N}) \tag{9e}$$

$$V_1(\tilde{x}_1(t)) \leq \rho'_{e,1},\ \ \forall\, t \in [t_k, t_{k+N}),\ \text{ if } \tilde{x}_1(t_k) \ \in\ \Omega_{\rho'_{e,1}} \tag{9f}$$

$$\frac{\partial V_1(\tilde{x}_1(t_k))}{\partial x} f_1(\tilde{x}_1(t_k), u_1(t_k), 0) \leq \frac{\partial V_1(\tilde{x}_1(t_k))}{\partial x}\ f_1(\tilde{x}_1(t_k), h_1(\tilde{x}_1(t_k)), 0),\ \text{ if }\ \tilde{x}_1(t_k) \in \Omega_{\rho_1}/\Omega_{\rho'_{e,1}} \tag{9g}$$

where $\tilde{x}_{b,1}(t_k)$ is used, with slight abuse of notation, to reflect the state measurement in deviation variable form from the operating steady-state.

The j-th LEMPC, $j > 1$, which is used for $t \in [t_{s,j}, t_{e,j})$, is formulated as follows:

$$\min_{u_j(t) \in S(\Delta)} \int_{t_k}^{t_{k+N}} L_e(\tilde{x}_j(\tau), u_j(\tau))\, d\tau \tag{10a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}_j(t) = f_j(\tilde{x}_j(t), u_j(t), 0) \tag{10b}$$

$$\tilde{x}_j(t_k) = \tilde{x}_{b,j}(t_k) \tag{10c}$$

$$\tilde{x}_j(t) \in X_j,\ \forall\, t \in [t_k, t_{k+N}) \tag{10d}$$

$$u_j(t) \in U_j,\ \ \forall\, t \in [t_k, t_{k+N}) \tag{10e}$$

$$\frac{\partial V_j(\tilde{x}_j(t_k))}{\partial x} f_j(\tilde{x}_j(t_k), u_j(t_k), 0) \leq \frac{\partial V_j(\tilde{x}_j(t_k))}{\partial x}\ f_j(\tilde{x}_j(t_k), h_j(\tilde{x}_j(t_k)), 0) \tag{10f}$$

where $\tilde{x}_{b,j}(t_k)$ represents the state measurement in deviation variable form from the j-th steady-state. A state measurement cyberattack on Eqs. 9-10 could cause $\tilde{x}_{b,1}(t_k)$ in Eq. 9c and $\tilde{x}_{b,j}(t_k)$ in Eq. 10c to not necessarily be reflective of the actual process state.

Randomized LEMPC Changes to Probe for Cyberattacks: Implementation Strategy

The implementation strategy for this detection method is as follows, and includes a region $\Omega_{\rho_{samp2,1}}$, which will be clarified in Section "Randomized LEMPC Changes to Probe for Cyberattacks: Stability and Feasibility Analysis" and is chosen such that if the actual state is in $\Omega_{\rho_{samp2,1}} \subset \Omega_{\rho_1}$, under sufficient conditions, then the closed-loop state and the state measurement are maintained in Ω_{ρ_1} for $t \geq 0$:

1. At a sampling time t_k, the 1-LEMPC receives the state measurement $\tilde{x}_{b,j}(t_k)$. Go to Step 2.
2. At t_k, an index ζ is set to a random number. If this number falls within a range that has been selected to initiate probing for cyberattacks, randomly generate a j-th steady-state ($j > 1$) with a stability region $\Omega_{\rho_j} \subset \Omega_{\rho_{samp2,1}}$ that has a steady-state input within the input bounds and contains the state measurement $\tilde{x}_{b,j}(t_k)$ (and where $\tilde{x}_{b,j}(t_k) \in \Omega_{\rho_{h,j}} \subset \Omega_{\rho_j} \subset \Omega_{\rho_{samp2,1}}$, which will be also clarified in Section "Randomized LEMPC Changes to Probe for Cyberattacks: Stability and Feasibility Analysis" and $\Omega_{\rho_{h,j}}$ is selected such that if the state measurement at t_k is in $\Omega_{\rho_{h,j}}$, under sufficient conditions, then the closed-loop state and the state measurement are maintained in Ω_{ρ_j} for $t \geq 0$, with the measured value of the state not in a neighborhood $\Omega_{\rho_{s,j}} \subset \Omega_{\rho_{h,j}}$ of the origin of the j-th steady-state). Set $t_{s,j} = t_k$, select $t_{e,j} = t_{k+1}$, and go to Step 4. Otherwise, if the value of ζ falls in a range which has not been selected to initiate probing for cyberattacks or the generation of a j-th steady-state meeting the conditions above is not possible, go to Step 3.
3. If $\tilde{x}_{b,j}(t_k) \in \Omega_{\rho'_{e,1}}$, go to Step 3a. Else, go to Step 3b.
   (a) Compute a control action for the subsequent sampling period with Eq. 9f of the 1-LEMPC activated. Go to Step 6.
   (b) Compute a control action for the subsequent sampling period with Eq. 9g of the 1-LEMPC activated. Go to Step 6.
4. The j-LEMPC receives the state measurement $\tilde{x}_{b,j}(t_k)$ and controls the process according to Eq. 10. Evaluate the Lyapunov function throughout the sampling period. If V_j does not decrease over the sampling period following $t_{s,j}$, detect that the process is potentially under a cyberattack and mitigating actions may be applied (e.g., a backup policy such as the use of redundant sensors or an emergency shut-down mode). Go to Step 5.
5. At $t_{e,j}$, switch back to operation under the 1-LEMPC. Go to Step 6.
6. Go to Step 1 ($k \leftarrow k + 1$).

Remark 2. Though it is possible to set $t_{e,j}$ to a value other than t_{k+1}, this may have several disadvantages: 1) it would cause the process to operate under a control law that is not the desired control law for normal operation for a longer period of time, potentially impacting profits; and 2) if the LEMPC of Eq. 10 is applied for a sufficient number of sampling periods, the closed-loop state would enter a neighborhood $\Omega_{\rho'_{s,j}}$ in which the value of V_j is no longer guaranteed to decrease. This could obscure the detection mechanism.

Remark 3. Both the random switching to and the generation of the j-LEMPC's are considered helpful. If, for example, only the time of switching was randomized (i.e., there were only a 1-LEMPC and a 2-LEMPC which could be activated at random times), an attacker may learn which control laws are possible and subsequently attempt to provide false state measurements that indicate that both V_1 and V_2 decrease over time so that regardless of whether the 1 or 2-LEMPC is activated, the attack is not detected via the probing mechanism. If the switching time was not fully randomized (e.g., probing was only performed when it would be less impactful on the economics than probing would be from another state), this would also add a level of determinism to the policy that has potential to be exploited by an attacker.

Randomized LEMPC Changes to Probe for Cyberattacks: Stability and Feasibility Analysis

In this section, we prove recursive feasibility and closed-loop stability of the process of Eq. 1 under the LEMPC of Eqs. 9-10. The impacts of bounded process noise and disturbances on the process state trajectory are characterized in Proposition 1 below, and Proposition 2 provides a bound on the value of the Lyapunov function evaluated at different points in the stability region.

Proposition 1. [21,20] *Consider the systems below*

$$\dot{x}_{b,j} = f_j(x_{b,j}(t), u_j(t), w(t)) \tag{11a}$$

$$\dot{\tilde{x}}_{b,j} = f_j(\tilde{x}_{b,j}(t), u_j(t), 0) \tag{11b}$$

with initial states $|x_{b,j}(t_0) - \tilde{x}_{b,j}(t_0)| \leq \delta$ *with* $t_0 = 0$. *If* $x_{b,j}(t), \tilde{x}_{b,j}(t) \in \Omega_{\rho_j}$ *for* $t \in [0, T]$, *then there exists a function* $f_{W,j}(\cdot, \cdot)$ *such that:*

$$|x_{b,j}(t) - \tilde{x}_{b,j}(t)| \leq f_{W,j}(\delta, t - t_0) \tag{12}$$

for all $x_{b,j}(t), \tilde{x}_{b,j}(t) \in \Omega_{\rho_j}$*,* $u_j \in U_j$*, and* $w \in W$*, with*

$$f_{W,j}(s,\tau) := \left(s + \frac{L_{w,j}\theta_w}{L_{x,j}}\right) e^{L_{x,j}\tau} - \frac{L_{w,j}\theta_w}{L_{x,j}} \tag{13}$$

Proposition 2. [21] *Consider the Lyapunov function* $V_j(\cdot)$ *of the nominal system of Eq. 1, in deviation variable form from the* j*-th steady-state, under the controller* $h_j(\cdot)$ *that satisfies Eqs. 2a-2d and 3 for the model of Eq. 1 in deviation variable form from the* j*-th steady-state. There exists a quadratic function* $f_{V_j}(\cdot)$ *such that:*

$$V_j(\bar{x}) \le V_j(\bar{x}') + f_{V_j}(|\bar{x} - \bar{x}'|) \tag{14}$$

for all $\bar{x}, \bar{x}' \in \Omega_{\rho_j}$ *with*

$$f_{V_j}(s) := \alpha_{4,j}(\alpha_{1,j}^{-1}(\rho_j))s + M_{v,j}s^2 \tag{15}$$

where $M_{v,j}$ *is a positive constant.*

The following theorem guarantees closed-loop stability of the process of Eq. 1 under the implementation strategy of Section "Randomized LEMPC Changes to Probe for Cyberattacks: Implementation Strategy" when no cyberattack occurs (i.e., with probing, but no attacks, so that the maximum value of δ in Proposition 1 would be θ'_v, where θ'_v represents the value of $\theta_{v,i}$ for Eq. 6 when $y_i(t) = x(t)$ (i.e., for full state measurement)).

Theorem 1. *Consider the closed-loop system of Eq. 1 under the implementation strategy of Section "Randomized LEMPC Changes to Probe for Cyberattacks: Implementation Strategy" and in the absence of a false sensor measurement cyberattack where each controller* $h_i(\cdot)$*,* $i \ge 1$*, used in each* i*-LEMPC meets the inequalities in Eqs. 2a-2d and 3 with respect to the* i*-th dynamic model. Let* $\epsilon_{W_i} > 0$*,* $\Delta > 0$*,* $N \ge 1$*,* $\Omega_{\rho_j} \subset \Omega_{\rho_{samp2,1}} \subset \Omega_{\rho_1} \subset X_1$ *for* $j > 1$*,* $\rho_j > \rho_{h,j} > \rho_{\min,j} > \rho_{s,j} > \rho'_{s,j} > 0$*, where* $\Omega_{\rho_{h,j}}$ *is defined as a level set of* Ω_{ρ_j} *that guarantees that if* $V_j(\tilde{x}_{b,j}(t_k)) \le \rho_{h,j}$*,* $V_j(x_{b,j}(t_k)) \le \rho_j$*, and* $\rho_1 > \rho_{samp2,1} > \rho_{samp,1} > \rho'_{e,1} > \rho_{\min,1} > \rho_{s,1} > \rho'_{s,1} > 0$*, where* $\Omega_{\rho_{samp,1}}$ *is defined as a level set of* Ω_{ρ_1} *where if* $x_{b,1}(t_k) \in \Omega_{\rho_1}/\Omega_{\rho_{samp,1}}$*,* $\tilde{x}_{b,1}(t_k) \in \Omega_{\rho_1}/\Omega_{\rho'_{e,1}}$*, satisfy:*

$$-\alpha_{3,i}(\alpha_{2,i}^{-1}(\rho'_{s,i})) + L'_{x,i}M_{f,i}\Delta \le -\epsilon_{w,i}/\Delta,\ i = 1, 2, \ldots \tag{16}$$

$$\rho'_{e,1} + f_{V,1}(f_{W,1}(\delta, \Delta)) \le \rho_{samp2,1} \tag{17}$$

$$-\alpha_{3,1}(\alpha_{2,1}^{-1}(\rho'_{e,1})) + L'_{x,1}M_{f,1}\Delta + L'_{x,1}\delta + L'_{w,1}\theta_w \leq -\epsilon'_{w,1}/\Delta \tag{18}$$

$$-\alpha_{3,j}(\alpha_{2,j}^{-1}(\rho_{s,j})) + L'_{x,j}M_{f,j}\Delta + L'_{x,j}\delta + L'_{w,j}\theta_w \leq -\epsilon'_{w,j}/\Delta,\ j = 1, 2, 3, \ldots \tag{19}$$

$$\rho_{\min,i} = \max\{V_i(x_{b,i}(t+\Delta)) : x_{b,i}(t) \in \Omega_{\rho'_{s,i}}\},\ i = 1, 2, \ldots \tag{20}$$

$$\rho_{samp2,1} \geq \max\{V_1(x_{b,1}(t+\Delta)) : x_{b,1}(t) \in \Omega_{\rho_{samp,1}}/\Omega_{\rho'_{e,1}}\} \tag{21}$$

$$\rho_1 \geq \max\{V_1(\tilde{x}_{b,1}(t_k)) : x_{b,1}(t_k) \in \Omega_{\rho_{samp2,1}}\} \tag{22}$$

$$\rho_j \geq \max\{V_j(\tilde{x}_{b,1}(t_k)) : \tilde{x}_{b,j}(t_k) \in \Omega_{\rho_{h,j}}\},\ j = 2, 3, \ldots \tag{23}$$

$$\rho'_{s,i} < \min\{V_i(x_{b,i}(t_k)) : \tilde{x}_{b,i}(t_k)\ \in \Omega_{\rho_{s,i}}\},\ i = 1, 2, \ldots \tag{24}$$

If $\tilde{x}_{b,1}(t_0) \in \Omega_{\rho_{samp2,1}}$, $x_{b,1}(t_0) \in \Omega_{\rho_{samp2,1}}$, and $|\tilde{x}_{b,i}(t_k) - x_{b,i}(t_k)| \leq \delta$, $k = 0, 1 \ldots$, then the closed-loop state is maintained in $\Omega_{\rho_{samp2,1}}$ and the state measurement is in Ω_{ρ_1} when the 1-LEMPC is activated at t_0 and for $t_{e,j-1} \leq t < t_{s,j}$, or when the j-LEMPC is activated for $t_{s,j} \leq t < t_{e,j}$ under the implementation strategy of Section "Randomized LEMPC Changes to Probe for Cyberattacks: Implementation Strategy," and the closed-loop state and the state measurement are maintained within Ω_{ρ_1} for $t \geq 0$. Furthermore, in the sampling period after $t_{s,j}$, if $\tilde{x}_{b,j}(t_k) \in \Omega_{\rho_j}/\Omega_{\rho_{s,j}}$, V_j decreases and $x(t) \in \Omega_{\rho_j}$ for $t \in [t_k, t_{k+1})$.

Proof. The proof consists of five parts. In the first part, recursive feasibility at every sampling time under the implementation strategy is demonstrated. In the second part, it is demonstrated that the closed-loop state and state measurement are maintained within Ω_{ρ_1} when the 1-LEMPC is used. In the third part, it is shown that the closed-loop state and state measurement are maintained within Ω_{ρ_j} when the j-LEMPC is used under the implementation strategy of Section "Randomized LEMPC Changes to Probe for Cyberattacks: Implementation Strategy." In the fourth part, it is demonstrated that the closed-loop state and state measurement are always contained within Ω_{ρ_1} under the proposed implementation strategy. Finally, in the fifth part, it is shown that in the sampling period after $t_{s,j}$, V_j decreases.

Part 1. Both the LEMPC of Eq. 9 and that of Eq. 10 must be feasible whenever they are activated according to the implementation strategy of Section "Randomized LEMPC Changes to Probe for Cyberattacks: Implementation Strategy." For both, h_j implemented in sample-and-hold is a feasible input policy. Specifically, when the 1-LEMPC is activated, the closed-loop state is in Ω_{ρ_1}, as will be proven below (Part 2). h_1 meets Eq. 9e from Eq. 2d and trivially satisfies Eq. 9g. Under the conditions in Eqs. 16 and 20, h_1 satisfies Eq. 9f if $\tilde{x}_{b,1}(t_k) \in \Omega_{\rho_1}$[24] (and thereby Eq. 9d since $\Omega_{\rho_1} \subset X_1$). Specifically, from Eq. 2b:

$$\frac{\partial V_1(\tilde{x}_{b,1}(t_p))}{\partial x} f_1(\tilde{x}_{b,1}(t_p), h_1(\tilde{x}_{b,1}(t_p)), 0) \leq -\alpha_{3,1}(|\tilde{x}_{b,1}(t_p)|),\ p = k, \ldots, k+N-1 \tag{25}$$

Therefore, for $t \in [t_p, t_{p+1})$ and $p = k, \ldots, k+N-1$ and $\tilde{x}_{b,1}(t_p) \in \Omega_{\rho'_{e,1}} / \Omega_{\rho'_{s,1}}$:

$$\frac{\partial V_1(\tilde{x}_{b,1}(t))}{\partial x} f_1(\tilde{x}_{b,1}(t), h_1(\tilde{x}_{b,1}(t_p)), 0) \leq -\alpha_{3,1}(\alpha_{2,1}^{-1}(\rho'_{s,1})) + L'_{x,1} M_{f,1} \Delta \tag{26}$$

where this inequality follows from adding and subtracting $\frac{\partial V_1(\tilde{x}_{b,1}(t_p))}{\partial x} f_1(\tilde{x}_{b,1}(t_p), h_1(\tilde{x}_{b,1}(t_p)), 0)$ to/from $\frac{\partial V_1(\tilde{x}_{b,1}(t))}{\partial x} f_1(\tilde{x}_{b,1}(t), h_1(\tilde{x}_{b,1}(t_p)), 0)$ and applying the triangle inequality, and subsequently using Eqs. 2a, 4b, and 5. If Eq. 16 holds, $\frac{\partial V_1(\tilde{x}_{b,1}(t))}{\partial x} f_1(\tilde{x}_{b,1}(t), h_1(\tilde{x}_{b,1}(t_p)), 0)$ is negative such that $V_1(t) \leq V_1(t_p)$ for $t \in [t_p, t_{p+1})$ so that if $\tilde{x}_{b,1}(t_p) \in \Omega_{\rho'_{e,1}}$, then $\tilde{x}_{b,1}(t) \in \Omega_{\rho'_{e,1}}$, $\forall\ t \in [t_p, t_{p+1})$. If instead $\tilde{x}_{b,1}(t_p) \in \Omega_{\rho'_{s,1}}$, then from Eq. 20 and $\rho'_{e,1} > \rho_{\min,1} > \rho_{s,1} > \rho'_{s,1}$, $\tilde{x}_{b,1}(t) \in \Omega_{\rho_{\min,1}} \subset \Omega_{\rho'_{e,1}}$ for $t \in [t_p, t_{p+1})$, as required by the constraint of Eq. 9f.

When instead the LEMPC utilized at a sampling time is the j-LEMPC of Eq. 10, the implementation strategy of Section "Randomized LEMPC Changes to Probe for Cyberattacks: Implementation Strategy" requires that $\tilde{x}_{b,j}(t_k) \in \Omega_{\rho_{h,j}} \subset \Omega_{\rho_j}$ and $x_{b,j}(t_k) \in \Omega_{\rho_j}$. Through the same arguments as for the 1-LEMPC (except that there is no constraint of the form of Eq. 9f), h_j in sample-and-hold is a feasible solution to Eq. 10.

Part 2. To demonstrate the case when the 1-LEMPC is used, we divide the proof into four cases: Case 1) the actual process state at t_0 ($x_{b,1}(t_0)$) is $x_{b,1}(t_0) \in \Omega_{\rho'_{e,1}}$ and the state measurement at t_0 (i.e., $\tilde{x}_{b,1}(t_0)$) is $\tilde{x}_{b,1}(t_0) \in \Omega_{\rho'_{e,1}}$; Case 2) $x_{b,1}(t_0) \in \Omega_{\rho_{samp2,1}} / \Omega_{\rho'_{e,1}}$ and $\tilde{x}_{b,1}(t_0) \in \Omega_{\rho_1} / \Omega_{\rho'_{e,1}}$; Case 3) $x_{b,1}(t_0) \in \Omega_{\rho_{samp,1}} / \Omega_{\rho'_{e,1}}$ but $\tilde{x}_{b,1}(t_0) \in \Omega_{\rho'_{e,1}}$; and Case 4) $x_{b,1}(t_0) \in \Omega_{\rho'_{e,1}}$ but $\tilde{x}_{b,1}(t_0) \in \Omega_{\rho_1} / \Omega_{\rho'_{e,1}}$.

Part 2 Case 1. If the state measurement used by the LEMPC is $\tilde{x}_{b,1}(t_0) \in \Omega_{\rho'_{e,1}}$, from Eq. 9f, $V_1(\tilde{x}_{b,1}(t_1)) \leq \rho'_{e,1}$. From Propositions 1 and 2, if $x_{b,1}(t_1) \in \Omega_{\rho_{samp2,1}}$, then:

$$V_1(x_{b,1}(t_1)) \leq V_1(\tilde{x}_{b,1}(t_1)) + f_{V,1}(|\tilde{x}_{b,1}(t_1) - x_{b,1}(t_1)|) \leq \rho'_{e,1} + f_{V,1}(f_{W,1}(\delta, \Delta)) \tag{27}$$

The assumption that $x_{b,1}(t_1) \in \Omega_{\rho_{samp2,1}}$ then follows from Eq. 17.

Part 2 Case 2. If $\tilde{x}_{b,1}(t_0) \in \Omega_{\rho_1}/\Omega_{\rho'_{e,1}}$ is the state measurement, Eq. 9g and Eq. 2b give:

$$\frac{\partial V_1(\tilde{x}_{b,1}(t_0))}{\partial x} f_1(\tilde{x}_{b,1}(t_0), u_1^*(t_0), 0) \leq -\alpha_{3,1}(|\tilde{x}_{b,1}(t_0)|) \tag{28}$$

where $u_i^*(t_0)$ is the optimal solution of the i-LEMPC at t_0. The time derivative of V_1 along the closed-loop state trajectories of $x_{b,1}$ from t_0 to t_1 satisfies:

$$\frac{\partial V_1(x_{b,1}(\tau))}{\partial x} f_1(x_{b,1}(\tau), u_1^*(t_0), w(\tau)) \leq -\alpha_{3,1}(\alpha_{2,1}^{-1}(\rho'_{e,1})) + L'_{x,1}M_{f,1}\Delta + L'_{x,1}\delta + L'_{w,1}\theta_w \tag{29}$$

which follows from adding and subtracting $\frac{\partial V_1(\tilde{x}_{b,1}(t_0))}{\partial x} f_1(\tilde{x}_{b,1}(t_0), u_1^*(t_0), 0)$ from $\frac{\partial V_1(x_{b,1}(\tau))}{\partial x} f_1(x_{b,1}(\tau), u_1^*(t_0), w(\tau))$ and using Eq. 28, the triangle inequality, the definition of $\tilde{x}_{b,1}(t_0)$, Eq. 5, Eq. 2a, and the fact that $\tilde{x}_{b,1}(t_0) \in \Omega_{\rho_1}/\Omega_{\rho'_{e,1}}$. If Eq. 18 holds, then $\dot{V}_1(x_{b,1}(\tau)) \leq -\epsilon'_{w,1}/\Delta$ for $\tau \in [t_0, t_1)$, so that $V_1(x_{b,1}(t)) \leq V_1(x_{b,1}(t_0))$, $\forall\ t \in [t_0, t_1)$, and thus $x_{b,1}(t) \in \Omega_{\rho_{samp2,1}}$.

Part 2 Case 3. If $x_{b,1}(t_0) \in \Omega_{\rho_{samp,1}}/\Omega_{\rho'_{e,1}}$, then from Eq. 21, $V_1(x_{b,1}(t)) \leq \rho_{samp2,1}$, $\forall\ t \in [t_0, t_1)$.

Part 2 Case 4. If the actual state $x_{b,1}(t_0) \in \Omega_{\rho'_{e,1}}$ and the state measurement $\tilde{x}_{b,1}(t_0) \in \Omega_{\rho_1}/\Omega_{\rho'_{e,1}}$ is provided to the LEMPC, Eq. 9g is enforced. From the proof for Case 2, this causes $V_1(x_{b,1}(t)) \leq V_1(x_{b,1}(t_0))$, $\forall\ t \in [t_0, t_1)$ if Eq. 18 holds and $x_{b,1}(t_0) \in \Omega_{\rho'_{e,1}}/\Omega_{\rho_{s,1}}$, such that $V_1(x_{b,1}(t)) \leq \rho_{samp2,1}$, $\forall\ t \in [t_0, t_1)$. If $x_{b,1}(t_0) \in \Omega_{\rho'_{s,1}}$, then $x_{b,1}(t) \in \Omega_{\rho_{\min,1}} \subset \Omega_{\rho_{samp2,1}}$, for $t \in [t_0, t_1)$, from Eq. 20.

Part 2 Cases 2-4 indicate that if $x_{b,1}(t_0) \in \Omega_{\rho_{samp2,1}}$, then $x_{b,1}(t) \in \Omega_{\rho_{samp2,1}}$ for $t \in [t_0, t_1)$. Applying this recursively, $x_{b,1}$ stays within $\Omega_{\rho_{samp2,1}}$ throughout the time period that the 1-LEMPC is used. Then, Eq. 22 indicates that the state measurement is always in Ω_{ρ_1}.

Part 3. When the j-LEMPC is used (for $j > 1$) (i.e., $\tilde{x}_{b,j}(t_k)$ must be in $\Omega_{\rho_{h,j}} \subset \Omega_{\rho_j} \subset \Omega_{\rho_{samp2,1}}$ with $x_{b,j}(t_k) \in \Omega_{\rho_j}$ by the implementation strategy of Section "Randomized LEMPC Changes to Probe for Cyberattacks: Implementation Strategy" and Eq. 23), if $\tilde{x}_{b,j}(t_k) \in \Omega_{\rho_{h,j}}/\Omega_{\rho_{s,j}}$, $j > 1$ (as required in Section ""Randomized LEMPC Changes to Probe for Cyberattacks: Implementation Strategy"), is the state measurement used by the LEMPC according to the implementation strategy of Section "Randomized LEMPC Changes to Probe for Cyberattacks: Implementation Strategy," Eqs. 10f and Eq. 2b give:

$$\frac{\partial V_j(\tilde{x}_{b,j}(t_k))}{\partial x} f_j(\tilde{x}_{b,j}(t_k), u_j^*(t_k), 0) \leq -\alpha_{3,j}(|\tilde{x}_{b,j}(t_k)|) \tag{30}$$

Following a similar procedure as in Part 2 Case 2, the time derivative of V_j along the closed-loop state trajectory of $x_{b,j}$ from t_k to t_{k+1} satisfies the following:

$$\frac{\partial V_j(x_{b,j}(\tau))}{\partial x} f_j(x_{b,j}(\tau), u_j^*(t_k), w(\tau)) \leq -\alpha_{3,j}(\alpha_{2,j}^{-1}(\rho_{s,j})) + L'_{x,j} M_{f,j} \Delta + L'_{x,j} \delta + L'_{w,j} \theta_w \tag{31}$$

which follows from adding and subtracting $\frac{\partial V_j(\tilde{x}_{b,j}(t_k))}{\partial x} f_j(\tilde{x}_{b,j}(t_0), u_j^*(t_k), 0)$ to and from $\frac{\partial V_j(x_{b,j}(\tau))}{\partial x} f_j(x_{b,j}(\tau), u_j^*(t_k), w(\tau))$ and using Eq. 30, the triangle inequality, the definition of $\tilde{x}_{b,j}(t_k)$, Eq. 5, Eq. 2a, and the fact that $x_{b,j}(t_k) \in \Omega_{\rho_{h,j}}/\Omega_{\rho_{s,j}}$ with the contractive constraint of Eq. 10f always activated and Eq. 24. If Eq. 19 holds, then $\dot{V}_j(x_{b,j}(\tau)) \leq -\epsilon'_{w,j}/\Delta$ for $\tau \in [t_k, t_{k+1})$, so that $V_j(x_{b,j}(t)) \leq V_j(x_k)$, $\forall\ t \in [t_k, t_{k+1})$, and thus $x_{b,j}(t) \in \Omega_{\rho_j} \subset \Omega_{\rho_{samp2,1}}$.

Part 4. To demonstrate that the closed-loop state is always maintained within $\Omega_{\rho_{samp2,1}}$ and that the measurement is always contained in Ω_{ρ_1} under the implementation strategy of Section "Randomized LEMPC Changes to Probe for Cyberattacks: Implementation Strategy," we proceed by induction. Consider first the conditions at t_0. At t_0, $x(t_0) \in \Omega_{\rho_{samp2,1}}$, and Eq. 22 guarantees that the state measurement is within Ω_{ρ_1}. Part 2 guarantees that $x(t_1) \in \Omega_{\rho_{samp2,1}}$ and that the state measurement at t_1 is within Ω_{ρ_1} once again. At t_k, $k > 0$, either the 1-LEMPC (if Eq. 9 is activated) or a j-LEMPC (if Eq. 10 is randomly selected to be activated) is used. If the 1-LEMPC is used, Part 2 guarantees that $x_{b,j}(t_{k+1}) \in \Omega_{\rho_{samp2,1}}$ and that the measurement at t_{k+1} is contained in Ω_{ρ_1}. If instead the j-LEMPC is used, then $x_{b,j}(t_k) \in \Omega_{\rho_j} \subset \Omega_{\rho_{samp2,1}}$ or else the implementation strategy of Section "Randomized LEMPC Changes to Probe for Cyberattacks: Implementation Strategy" would not have allowed the use of the j-LEMPC. When $x_{b,j}(t_k) \in \Omega_{\rho_j} \subset \Omega_{\rho_{samp2,1}}$ (by the conditions of the implementation strategy in Section "Randomized LEMPC Changes to Probe for Cyberattacks: Implementation Strategy"), Part 3 above guarantees that $x_{b,j}(t) \in \Omega_{\rho_j} \subset \Omega_{\rho_{samp2,1}}$, $\forall\ t \in [t_0, t_1]$ and that the measurement is in $\Omega_{\rho_j} \subset \Omega_{\rho_{samp2,1}}$, which is also a subset of Ω_{ρ_1} by the assumptions of the theorem. Therefore, at t_0, regardless of whether the 1-LEMPC or the j-LEMPC is activated, the closed-loop state is still within $\Omega_{\rho_{samp2,1}}$ and the state measurement is within Ω_{ρ_1} throughout the subsequent sampling period and at the subsequent sampling time. Applying this recursively indicates that the closed-loop state and state measurement are contained within $\Omega_{\rho_{samp2,1}}$ and Ω_{ρ_1}, respectively, at all times.

Part 5. Finally, we demonstrate that V_j, $j > 1$, decreases in a sampling period after $t_{s,j}$ by noting that the implementation strategy of Section "Randomized LEMPC Changes to Probe for Cyberattacks: Implementation Strategy" requires that the j-LEMPC only be activated if the actual state is within $\Omega_{\rho_j}/\Omega_{\rho'_{s,j}}$ (i.e., the measurement is within $\Omega_{\rho_{h,j}}/\Omega_{\rho_{s,j}}$, where $\Omega_{\rho_{s,j}}$ satisfies Eq. 24 and $\Omega_{\rho_{h,j}}$ satisfies Eq. 23). This ensures that the actual value of the state is outside of $\Omega_{\rho'_{s,j}}$ and within Ω_{ρ_j}. Therefore, because Eq. 19 holds for $x_{b,j}(t_k) \in \Omega_{\rho_j}/\Omega_{\rho'_{s,j}}$, the value of V_j will decrease for $t \in [t_k, t_{k+1})$. □

Remark 4. A number of regions are defined in the above theorem. Ω_{ρ_i}, $i = 1, 2, \ldots$ has been described as an invariant set in which it is desired to maintain the closed-loop state and state estimates, and $\Omega_{\rho'_{e,1}}$ is a region used in differentiating between whether Eq. 9f or 9g is used in Eq. 9). $\Omega_{\rho_{\min,i}}$, $i = 1, 2, \ldots$, is defined via Eq. 20 as the maximum value of V_i evaluated for the actual state that can be reached within a sampling period if the actual state is within $\Omega_{\rho'_{s,i}}$ at a sampling time, and any input in the input bounds is applied to the system. $\Omega_{\rho_{samp,1}}$ is defined as a region where, if the actual closed-loop state is within this region at a sampling time, the maximum distance that the closed-loop state would be able to go within a sampling period is into $\Omega_{\rho_{samp2,1}}$. $\Omega_{\rho_{samp,1}}$ is important to characterize due to the presence of measurement noise; specifically, in the presence of measurement noise, there may be some range of states outside of $\Omega_{\rho'_{e,1}}$ where it is still possible that with $|\tilde{x}_{b,j}(t_k) - x_{b,j}(t_k)| < \delta$, the measured state may be within $\Omega_{\rho'_{e,1}}$. In this case, under the 1-LEMPC, the constraint of Eq. 9f would be activated, though if the true state measurement was known, the constraint of Eq. 9g would be activated. To prevent this discrepancy from leading to closed-loop stability issues, $\Omega_{\rho_{samp,1}}$ is defined as a region within Ω_{ρ_1} where with the bound δ on the difference between the actual and measured values of the state, the measured state could still be within $\Omega_{\rho'_{e,1}}$. $\Omega_{\rho_{samp2,1}}$ is then defined to be within Ω_{ρ_1} so that the maximum distance that the closed-loop state could travel when the state measurement is within $\Omega_{\rho'_{e,1}}$ but the actual state is outside of it is still within Ω_{ρ_1}. Not only is the actual state then defined to be within Ω_{ρ_1} when the actual state is within $\Omega_{\rho_{samp2,1}}$, but the state measurement is then also required to be within Ω_{ρ_1} (Eq. 22). Furthermore, because Eqs. 9g and 10f only enforce a decrease condition on V_j, $j = 2, 3, \ldots$, when the closed-loop state is within $\Omega_{\rho_j}/\Omega_{\rho'_{s,j}}$, the implementation strategy of Section "Randomized LEMPC Changes to Probe for Cyberattacks: Implementation Strategy" requires that the actual value of the closed-loop state be outside of $\Omega_{\rho'_{s,j}}$. First, to guarantee that the actual state at t_k is inside Ω_{ρ_j}, we define the region $\rho_{h,j}$ in Eq. 23 as a within Ω_{ρ_j} such that if the state measurement is within $\Omega_{\rho_{h,j}}$ at t_k, the actual state value is inside Ω_{ρ_j}. However, due to measurement noise, the measured value may be outside of $\Omega_{\rho'_{s,j}}$, but the actual state may be within $\Omega_{\rho'_{s,j}}$, which could impact the ability of V_j to decrease over a sampling period following the activation of the constraint of Eq. 10f. To prevent this, we define the region $\Omega_{\rho_{s,j}}$ in Eq. 24 such that if the state measurement is within $\Omega_{\rho_{s,j}}$ at t_k, the actual state value is still outside of $\Omega_{\rho'_{s,j}}$ so that meeting the condition of Eq. 16 guarantees that V_j will decrease in the following sampling period.

Remark 5. According to the proof above, the LEMPC formulation is designed to account for sufficiently small disturbances and measurement noise. Therefore, the lack of a decrease in the Lyapunov function under the proposed control/detection strategy would not be due to plant/model mismatch or sensor noise if the conditions of Theorem 1 are met. Furthermore, if V_j does not decrease over a sampling period after $t_{s,j}$ when computed using the sensor measurements, this strategy detects the attack even if all sensors are compromised.

Remark 6. If the control law is changed at a sampling period, the attacker may try to detect this and determine which control law a given control action throughout a sampling period could have been derived from to attempt to ensure that the false state measurement that they provide at the beginning of the next sampling period causes the expected behavior of V_j. However, since the control action is being implemented in sample-and-hold over the sampling period, there is not much data on the control law available from u_i^* for the attacker then to work from. If the LEMPC is computing set-points for regulatory controllers, these controllers would not be providing more information on what control law (i.e., Lyapunov function) the LEMPC used. When measurements of the state are available more frequently than every sampling period, an attacker may not be able to falsify all of the measurements immediately after $t_{s,j}$ until they are aware of the change in the control law, which has potential to reveal the attack if V_j does not decrease for any fraction of the sampling period after $t_{s,j}$ due to this. However, Detection Strategy 1 has no guarantees that it will detect an attack. When an attack occurs, the sensor measurements are falsified, and that can compromise closed-loop stability before that attack is detected, and may also result in a false sensor measurement trajectory that happens to decrease V_j. There is no guarantee that a probing maneuver will be activated at a time when it could reveal an attack. The concept of the method is that it could be used to flag a false sensor measurement cyberattack if it does not cause V_j to decrease when it should be.

Remark 7. The worst-case rate at which V_j will decrease over a sampling period following activation of the j-LEMPC could be slow, in which case a practical sensor may not register the decrease in the value of the Lyapunov function even if it is occurring. Therefore, from a practical perspective, there could be cases where a sufficiently long period of time might be needed for the decrease in the Lyapunov function to be registered by a practical sensing device, and that amount of time may or may not be equivalent to one sampling period after the probing mechanism is triggered.

Randomized LEMPC Changes to Probe for Cyberattacks: Chemical Process Example

In this section, a chemical process example is used to demonstrate the implementation of Detection Strategy 1, as well as to highlight the limitation of this method in that it is not guaranteed to detect attacks. The nonlinear process model consists of a continuous stirred tank reactor (CSTR) with a second-order, exothermic, irreversible reaction of the form $A \rightarrow B$ with the following process dynamics:

$$\dot{C}_A = \frac{F}{V}(C_{A0} - C_A) - k_0 e^{-\frac{E}{R_g T}} C_A^2 \tag{32}$$

$$\dot{T} = \frac{F}{V}(T_0 - T) - \frac{\Delta H k_0}{\rho_L C_p} e^{-\frac{E}{R_g T}} C_A^2 + \frac{Q}{\rho_L C_p V} \tag{33}$$

where the states are the reactant concentration of species A and temperature in the reactor (C_A and T, respectively). The manipulated inputs are C_{A0} (the reactant feed concentration of species A) and the heat rate Q. The values of the parameters of the CSTR model (F, V, k_0, E, R_g, T_0, ρ_L, ΔH, and C_p) are taken from.[25] The vectors of deviation variables for the states and inputs from their operating steady-state values, $x_{1s} = [C_{As}\ T_s]^T = [1.22 \text{ kmol/m}^3\ 438.2 \text{ K}]^T$, $[C_{A0s}\ Q_s]^T = [4.0 \text{ kmol/m}^3\ 0 \text{ kJ/h}]^T$, respectively, are $x_1 = [x_{1,1}\ x_{1,2}]^T = [C_A - C_{As}\ T - T_s]^T$ and $u_1 = [u_{1,1}\ u_{1,2}]^T = [C_{A0} - C_{A0s}\ Q - Q_s]^T$. The process model represented by Eqs. 32-33 is numerically integrated using the explicit Euler method with integration step of 10^{-4} h. The economic stage cost is selected to be $L_e = k_0 e^{-E/(RT)} C_A^2$. Despite the simplicity of this case study, it is illustrative for the cyberattack detection methods without convoluting the results through a more complex example, and the theoretical results of this work hold in the case of more complex processes.

The controller receives a state measurement subject to bounded measurement noise and the process is subject to bounded disturbances. The noise is represented by a standard normal distribution with mean zero, standard deviations of 0.002 kmol/m^3 and 0.5 K, and bounds of 0.002 kmol/m^3 and 0.5 K for the concentration of the reactant and reactor temperature, respectively. Process disturbances were added to the right-hand side of the differential equations describing the rates of change of C_A and T with zero mean and standard deviations of 0.5 kmol/m^3 h and 2 K/h, and bounds of 2 kmol/m^3 h and 5 K/h, respectively. The baseline LEMPC formulation used Lyapunov-based stability constraints were designed using a Lyapunov function $V_1 = x_{b,1}^T P x_{b,1}$, where $P = [1200\ 5; 5\ 0.1]$. In the selected Lyapunov-based controller $h_1(x_{b,1}) = [h_{1,1}(x_{b,1})\ h_{1,2}(x_{b,1})]^T$, $h_{1,1}(x_{b,1})$ was set to 0 kmol/m^3 for simplicity and $h_{1,2}(x_{b,1})$ was designed via Sontag's control law.[26] The stability region was defined with $\rho_1 = 300$ (i.e., $\Omega_{\rho_1} = \{x_1 \in R^2 : V_1(x_{b,1}) \leq \rho_1\}$), and $\rho'_{e,1} = 225$. N and Δ were set to 10 and 0.01 h, respectively.

The process was simulated for 0.1 h of operation, initialized at $x_{1,init} = [x_{1,1}(t_0)\ x_{1,2}(t_0)]^T = [-0.21 \text{ kmol/m}^3\ 28.89 \text{ K}]^T$ in MATLAB R2016b using fmincon. In the LEMPC, the value of the decision variable corresponding to Q was scaled down by 10^5, and probing was initialized at t_0. Four simulations were performed: two in which the original steady-state and stability region were utilized for probing (i.e., a constraint of the form of Eq. 10f was enforced at the end of the first sampling period, and no constraint of the form in Eq. 9f was used), and two in which a modified steady-state and stability region were utilized for probing. The modified steady-state (x_{2s}) has a stability region in Ω_{ρ_1} and includes $x_{1,init}$. Specifically, the new steady-state was selected to be $x_{2s} = [1.22 \text{ kmol/m}^3\ 450 \text{ K}]^T$. The stability region around this new steady-state is defined using $V_2(x) = x_2^T P_2 x_2$, where $x_2 = x_1 + x_{1s} - x_{2s}$, with $P_2 = [2100\ 10; 10\ 0.25]$, and $\rho_2 = 100$ (i.e., $\Omega_{\rho_2} = \{x_2 \in R^2 : V_2(x_2) \leq \rho_2\}$). The modified LEMPC design was formulated with respect to x_2 and designed using a Lyapunov-based controller with $h_{2,1}(x_{b,2}) = 0$ kmol/m^3 and $h_{2,2}(x_{b,2})$ selected

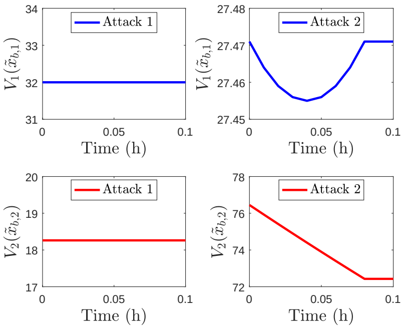

Figure 1: V_1 (top plots) and V_2 (bottom plots) profiles over 0.1 h of operation for the process example in the presence of different cyberattack policies.

using Sontag's control law with respect to $V_2(x_{b,2})$.

Two cyberattacks were simulated on the two different probing formulations: 1) Attack 1: A constant false state measurement $x_{1,1} = 0.1$ kmol/m^3, $x_{1,2} = 10$ K is provided to the LEMPC's starting at t_0; 2) Attack 2: A false state measurement of the form $x_{1,1} = -0.17$ kmol/m^3, $x_{1,2} = 8.0 + 0.1r$ K, with r increasing by one from 1 to 9 at each sampling time until the 9th sampling time and then keeping r at 9, is provided to the controller starting at t_0. The $V_1(\tilde{x}_{b,1})$ and $V_2(\tilde{x}_{b,2})$ profiles that result when the attacks and probing are both initialized at t_0 are presented in Fig. 1. It can be seen that under Attack 1, whether the value of V_1 or V_2 is monitored over time, the attack would be detected, whereas if the probing was only undertaken for a sampling period as suggested in the theory (it is applied for the entire 0.1 h simulation in Fig. 1), Attack 2 would not be detected with either probing strategy.

Remark 8. In general with the proposed method, until the probing starts, an LEMPC may not be driving a process toward the steady-state so that there would not necessarily be a decrease in the Lyapunov function expected over a sampling period before a probing maneuver.

Detection Strategy 2: Cyberattack-Mitigating State Feedback LEMPC

Detection Strategy 1 described in Section "Detection Strategy 1: Randomized LEMPC Changes to Probe for Cyberattacks" may identify a cyberattack by taking advantage of LEMPC's properties, but it does not guarantee closed-loop stability in the presence of an attack (and as shown in the example of the prior section, there can be many cases in which the method fails to detect attacks). A strategy suggested in[20, 17] could be used instead to give a detection strategy that provides short-term guarantees that the closed-loop state is maintained in a bounded region of operation after an attack on the sensor measurements (even, potentially, all of the measurements). Specifically, this second detection strategy uses state predictions from the process model from the last state measurement to identify an attack if the predictions deviate too significantly from the measurements. When the norm of the difference between the state measurement and the state prediction is above a threshold, the measurement is flagged as a possible sensor attack. When the difference is below a threshold, then even if the measurement was falsified, the closed-loop state can be maintained in Ω_{ρ_1} for a sampling period after the attack if the process is operated under an LEMPC with a sufficiently conservative design (if the attack is not detected at t_k, an auxiliary detection mechanism (e.g., machine learning detection methods[3]) could be used in addition to attempt to identify a cyberattack on the sensor measurements to avoid the potential that the closed-loop state may leave Ω_{ρ_1} after t_{k+1}). The developments below will focus on the case that the 1-LEMPC of Eq. 9 is used to control the process at all times.

Cyberattack-Mitigating State Feedback LEMPC: Implementation Strategy

The implementation strategy for this detection/control method is as follows, where $\tilde{x}_{b,1}(t_k|t_{k-1})$ denotes the prediction of the state $\tilde{x}_{b,1}$ at t_k evaluated by integrating the dynamic model of Eq. 9b from a measurement at t_{k-1} until t_k:

1. At sampling time t_k, if $|\tilde{x}_{b,1}(t_k|t_{k-1}) - \tilde{x}_{b,1}(t_k|t_k)| > \nu$, detect that a cyberattack is occurring and go to Step 1a. Else, go to Step 1b.
    (a) Apply a backup strategy or enter an emergency shut-down mode.
    (b) Operate the process under the LEMPC of Eq. 9 while employing an auxiliary detection mechanism to attempt to flag any un-detected attack at t_k. $t_k \leftarrow t_{k+1}$. Go to Step 1.

Cyberattack-Mitigating State Feedback LEMPC: Stability and Feasibility Analysis

The following theorem guarantees that in the presence of bounded measurement noise and disturbances, the implementation strategy of Section "Cyberattack-Mitigating State Feedback LEMPC: Implementation Strategy" maintains the closed-loop state within Ω_{ρ_1} before an attack occurs and for at least one sampling period after the attack.

Theorem 2. [20] *Consider the system of Eq. 1 in closed-loop under the implementation strategy of Section "Cyberattack-Mitigating State Feedback LEMPC: Implementation Strategy" based on a controller $h_1(\cdot)$ that satisfies the assumptions of Eqs. 2a-2d and 3. Let the conditions of Theorem 1 hold with $t_{s,j} = \infty$, $j = 2, 3, \ldots$, and $\delta \geq f_{W,1}(\theta'_v, \Delta) + \nu$. If $\tilde{x}_{b,1}(t_0) \in \Omega_{\rho_{samp2,1}} \subset \Omega_{\rho_1}$ and $x_{b,1}(t_0) \in \Omega_{\rho_{samp2,1}}$, then $x_{b,1}(t) \in \Omega_{\rho_{samp2,1}}$ and the state measurement at each sampling time is in Ω_{ρ_1} for all times before a sampling time t_A that a cyberattack falsifies a state measurement, and $x_{b,1}(t) \in \Omega_{\rho_{samp2,1}}$ for $t \in [t_A, t_A + \Delta)$, if the attack is not detected at t_A.*

Proof. Theorem 1 guarantees that $\tilde{x}_{b,1}(t) \in \Omega_{\rho_1}$ and $x_{b,1}(t) \in \Omega_{\rho_{samp2,1}}$ for $t < t_A$. To prove that $x_{b,1}(t) \in \Omega_{\rho_{samp2,1}}$ for $t \in [t_A, t_A + \Delta)$, consider the measurements $\tilde{x}_{b,1}(t_{k-1}|t_{k-1})$ and $\tilde{x}_{b,1}(t_k|t_k)$, and the predicted state $\tilde{x}_{b,1}(t|t_{k-1})$ from the nominal model of Eq. 9b for $t \in [t_{k-1}, t_k]$. From the bounded measurement noise assumption, $|\tilde{x}_{b,1}(t_{k-1}|t_{k-1}) - x_{b,1}(t_{k-1})| \leq \theta'_v$. Proposition 1 gives:

$$|x_{b,1}(t_k) - \tilde{x}_{b,1}(t_k|t_{k-1})| \leq f_{W,1}(\theta'_v, \Delta) \tag{34}$$

If an attack is not flagged at t_k:

$$\begin{aligned} |x_{b,1}(t_k) - \tilde{x}_{b,1}(t_k|t_k)| &\leq |x_{b,1}(t_k) - \tilde{x}_{b,1}(t_k|t_{k-1}) + \tilde{x}_{b,1}(t_k|t_{k-1}) - \tilde{x}_{b,1}(t_k|t_k)| \\ &\leq f_{W,1}(\theta'_v, \Delta) + |\tilde{x}_{b,1}(t_k|t_{k-1}) - \tilde{x}_{b,1}(t_k|t_k)| \leq f_{W,1}(\theta'_v, \Delta) + \nu \end{aligned} \tag{35}$$

where the last inequality follows from the fact that the implementation strategy would have flagged the attack at t_k if $|\tilde{x}_{b,1}(t_k|t_{k-1}) - \tilde{x}_{b,1}(t_k|t_k)| > \nu$. Finally, when δ in Theorem 1 satisfies $\delta \geq f_{W,1}(\theta'_v, \Delta) + \nu$, then the closed-loop state is maintained within $\Omega_{\rho_{samp2,1}}$ over the subsequent sampling period according to the proof of Theorem 1 if there is an attack at t_k. □

Remark 9. One could consider employing Detection Strategy 1 as an auxiliary detection mechanism with Detection Strategy 2 if the j-LEMPC is activated at the beginning of one of the sampling periods over which closed-loop stability is still maintained after an attack (but Detection Strategy 1 is not guaranteed to detect the attack).

Remark 10. The value of the threshold ν is a design decision that should be specified considering Eq. 35 and the conditions of Theorem 1. Specifically, larger values of ν require a more conservative stability region. However, overly conservative values could cause false alarms, since there is some difference between the state measurement and state prediction due to noise and disturbances.

Detection Strategy 3: Cyberattack-Resilient Output Feedback LEMPC

Detection Strategy 2 ensures that the closed-loop state is maintained in Ω_{ρ_1} for only one sampling period after an attack occurs. Detection Strategy 3, which guarantees that the closed-loop state is maintained in a bounded region of operation for all time, uses multiple redundant state estimators (where at least one cannot be impacted by the false sensor measurements) coupled with an output feedback LEMPC. This method extends the results in[19] by considering that multiple state estimators may be impacted by a cyberattack.

Cyberattack-Resilient Output Feedback LEMPC: Formulation

The output feedback LEMPC design used for this detection strategy is formulated to receive a state estimate z_1 from one of the redundant state estimators (the estimator used to provide state estimates to the LEMPC will be denoted as the $i = 1$ estimator) at t_k. The notation follows that of Eq. 8 with Eq. 8c replaced by $\tilde{x}(t_k) = z_1(t_k)$; we will subsequently refer to this LEMPC as the output feedback LEMPC of Eq. 8.

Detection Strategy 3 guarantees that any cyberattacks which would drive the closed-loop state out of Ω_ρ will be detected before this occurs. It recognizes cyberattacks by flagging deviations of the state estimates from "normal" behavior; however, as "normal" behavior includes both measurement noise and disturbances (Eqs. 1 and 6), care must be taken in setting the threshold on the state estimate deviation from a "normal" value to avoid false detections. With slight abuse of notation compared to that used in describing Detection Strategies 1 and 2, we here revert to the use of $x(t)$ (rather than $x_{b,j}(t)$)) to denote the actual state at time t. We consider that at least one of the M state estimators is not affected by false state measurements (i.e., up to $M - 1$ state estimators are receiving measurements for which at least some subset of them are falsified). To determine a threshold, we note that the bounds in Assumption 2 imply that the following holds:

$$\begin{aligned} |z_i(t) - z_j(t)| &= |z_i(t) - x(t) + x(t) - z_j(t)| \leq |z_i(t) - x(t)| + |z_j(t) - x(t)| \\ &\leq \epsilon_{ij} := (e^*_{mi} + e^*_{mj}) \leq \epsilon_{\max} := \max\{\epsilon_{ij}\} \end{aligned} \tag{36}$$

for all $i \neq j$, $i = 1, \ldots, M$, $j = 1, \ldots, M$, as long as $t \geq t_q = \max\{t_{b1}, \ldots, t_{bM}\}$. Therefore, abnormal behavior can be detected if $|z_i(t_k) - z_j(t_k)| > \epsilon_{\max}$ if $t_k > t_q$ (this avoids false detections). In practice, it may not be possible to know the numbers e^*_{mi} and e^*_{mj}, as they can only be known by knowing an upper bound on how far off each $z_i(t)$ is from $x(t)$, which may not be known since full state feedback may not be available. By using Eq. 36 with data from an attack-free scenario, a bound may be able to be placed on the possible value of $\epsilon_{\max}$ based on how far apart $z_i(t)$ and $z_j(t)$ are over time. In the following, we will assume that the upper bound $\epsilon_{\max}$ can be determined.

Cyberattack-Resilient Output Feedback LEMPC: Implementation Strategy

This implementation strategy assumes that the process has already been run successfully in the absence of attacks under the output feedback LEMPC of Eq. 8 for some time such that $|z_i(t)-x(t)| \leq \epsilon^*_{mi}$ for all $i = 1, \ldots, M$ before an attack:

1. At sampling time t_k, if $|z_i(t_k) - z_j(t_k)| > \epsilon_{\max}$, $i = 1, \ldots, M$, $j = 1, \ldots, M$, or $z_1(t_k) \notin \Omega_\rho$ (where z_1 is the state estimate used in the EMPC design), detect that a cyberattack is occurring and go to Step 1a. Else, go to Step 1b.
   (a) Enter an emergency shut-down mode that no longer operates the process under the output feedback LEMPC of Eq. 8.
   (b) Operate using the output feedback LEMPC of Eq. 8. $t_k \leftarrow t_{k+1}$. Go to Step 1.

Cyberattack-Resilient Output Feedback LEMPC: Stability and Feasibility Analysis

This section details feasibility and closed-loop stability results for systems of Eq. 1 under the implementation strategy of Section "Cyberattack-Resilient Output Feedback LEMPC: Implementation Strategy." We first present a proposition that bounds the worst-case difference between the state estimate used by the output feedback LEMPC of Eq. 8 and the actual value of the process state under the implementation strategy when an attack is not flagged.

Proposition 3. *Consider the system of Eq. 1 under the implementation strategy of Section "Cyberattack-Resilient Output Feedback LEMPC: Implementation Strategy" where $M > 1$ state estimators develop independent estimates of the process state and at least one of these estimators is not impacted by false state measurements being provided to the estimators (and the attacks do not begin until after t_q). If a false sensor measurement cyberattack is not flagged at t_k according to the implementation strategy, then the worst-case difference between z_1 and the actual state $x(t_k)$ is given by:*

$$|z_1(t_k) - x(t_k)| \leq \epsilon^*_M := \epsilon_{\max} + \max\{e^*_{mj}\},\ j = 1, \ldots, M \tag{37}$$

Proof. Two cases must be considered: Case 1) z_1 is not impacted by the attack; Case 2) z_1 is impacted by the attack.

Case 1. When z_1 is not impacted by an attack, $|z_1(t_k) - x(t_k)|$ is given by Assumption 2 for $t_k > t_q$. Specifically, Eq. 37 holds since:

$$|z_1(t_k) - x(t_k)| \leq e^*_{m1} \leq \epsilon_{\max} + \max(e^*_{mj}) = \epsilon^*_M \tag{38}$$

Case 2. When z_1 is impacted by an attack but at least one of the other estimators (with its estimate denoted as z_2) is not, the following upper bound can be developed:

$$\begin{aligned} |z_1(t_k) - x(t_k)| &= |z_1(t_k) - z_2(t_k) + z_2(t_k) - x(t_k)| \leq |z_1(t_k) - z_2(t_k)| + |z_2(t_k) - x(t_k)| \\ &\leq \epsilon_{\max} + \max(e^*_{mj}) = \epsilon^*_M, \ j = 1, \ldots, M \end{aligned} \tag{39}$$

where the last inequality follows from the fact that the detection algorithm was not activated (i.e., $|z_1(t_k) - z_2(t_k)| \leq \epsilon_{\max}$) and the assumption that the estimator producing z_2 is not impacted by the false sensor measurements (i.e., $|z_2(t_k) - x(t_k)| \leq \max(e^*_{mj})$), according to Assumption 2). □

Theorem 3 below summarizes the stability properties of the system of Eq. 1 operated under the proposed implementation strategy in Section "Cyberattack-Resilient Output Feedback LEMPC: Implementation Strategy." This theorem re-purposes a bound on the allowable error in a state estimate supplied to an output feedback-based LEMPC in the absence of cyberattacks from.[22,21] Specifically, the proposed cyberattack detection method enables the bound in Eq. 37 to be defined, which allows cyberattacks to be treated in the framework previously developed in[22,21] for guaranteeing closed-loop stability of output feedback LEMPC in the presence of measurement noise and disturbances, and thereby allows the combined detection and control framework to guarantee closed-loop stability when a cyberattack is not flagged according to the proposed methodology.

Theorem 3. *Consider the system of Eq. 1 in closed-loop under the LEMPC of Eq. 8 based on an observer and controller pair satisfying Assumptions 1-2 and formulated with respect to the $i = 1$ measurement vector, and formulated with respect to a controller $h(\cdot)$ that meets Eqs. 2a-2d and 3. Let the conditions of Proposition 3 hold, and $\theta_w \leq \theta^*_w$, $\theta_{v,i} \leq \theta^*_{v,i}$, $\epsilon_i \in (\epsilon^*_{Li}, \epsilon^*_{Ui})$, and $|z_i(t_0) - x(t_0)| \leq e_{m0i}$, for $i = 1, \ldots, M$. Also, let $\epsilon_{W,1} > 0$, $\Delta > 0$, $\Omega_\rho \subset X$, and $\rho > \rho_{\max} > \rho_{1,1} > \rho_{e,1} > \rho_{\min,1} >$*

$\rho_{s,1} > 0$, satisfy:

$$\rho_{e,1} \leq \rho_{\max} - \max\{f_V(f_W(\epsilon_M^*, \Delta)), M_f \max\{t_{z1}, \Delta\}\alpha_4(\alpha_1^{-1}(\rho_{\max}))\} \tag{40}$$

$$\rho_{e,1} \leq \rho - f_V(f_W(\epsilon_M^*, \Delta)) - f_V(\epsilon_M^*) \tag{41}$$

$$-\alpha_3(\alpha_2^{-1}(\rho_{s,1})) + L_x'(M_f\Delta + \epsilon_M^*) + L_w'\theta_w \leq -\epsilon_{W,1}/\Delta \tag{42}$$

$$\rho_{\min,1} = \max\{V(x(t+\Delta))|V(x(t)) \leq \rho_{s,1}\} \tag{43}$$

$$\rho_{\min,1} + f_V(f_W(\epsilon_M^*, \Delta)) \leq \rho \tag{44}$$

$$\rho_{\max} + f_V(\epsilon_M^*) \leq \rho \tag{45}$$

where t_{z1} is the first sampling time after t_{b1}, and f_V and f_W are defined as in Propositions 1 and 2 but with the subscripts dropped. Then, if $x(t_0) \in \Omega_{\rho_{e,1}}$, $x(t) \in \Omega_{\rho_{\max}}$ for all $t \geq 0$ and $z_1(t_h) \in \Omega_\rho$ for $t_h \geq \max\{\Delta, t_{z1}\}$ until a cyberattack is detected according to the implementation strategy in Section "Cyberattack-Resilient Output Feedback LEMPC: Implementation Strategy," if the attack occurs after t_q.

Proof. The proof consists of four parts. In Part 1, feasibility of the output feedback LEMPC of Eq. 8 is proven when $z_1(t_k) \in \Omega_\rho$. In Part 2, we prove that the closed-loop state trajectory is contained in $\Omega_{\rho_{\max}}$ for $t \in [t_0, \max\{\Delta, t_{z1}\})$. In Part 3, we prove that for $t \geq \max\{\Delta, t_{z1}\}$ but before an attack occurs, $x(t)$ is bounded within $\Omega_{\rho_{\max}}$ and $z_1(t)$ is bounded within Ω_ρ. In Part 4, we prove that if there is an attack at t_k but it is not detected using the proposed methodology (i.e., $|z_i(t) - z_j(t)| \leq \epsilon_{\max}$, for all $i = 1, \ldots, M$, $j = 1, \ldots, M$), $x(t)$ is bounded in $\Omega_{\rho_{\max}}$ and $z_1(t)$ is bounded in Ω_ρ.

Part 1. The Lyapunov-based controller $h(x)$ implemented in sample-and-hold is a feasible solution to the output feedback LEMPC of Eq. 8 when $\tilde{x}(t_k) = z_1(t_k) \in \Omega_\rho$. Specifically, $h(x(t_p))$, $p = k, \ldots, k+N-1$, $t \in [t_p, t_{p+1})$, is a feasible solution to the output feedback LEMPC of Eq. 8 because it meets the input constraints of Eq. 8e according to Eq. 2, it meets the state constraints of Eq. 8d when $\tilde{x}(t) \in \Omega_\rho \subset X$, it trivially satisfies Eq. 8g, and it satisfies Eq. 8f because the region $\Omega_{\rho_{e,1}}$ is forward invariant under h implemented in a sample-and-hold fashion when $\rho_{e,1} > \rho_{\min,1}$, due to the closed-loop stability properties of the Lyapunov-based controller (as noted in the proof of Part 1 for Theorem 1).

Part 2. To demonstrate boundedness of the closed-loop state in $\Omega_{\rho_{\max}}$ for $t \in [t_0, \max\{\Delta, t_{z1}\})$, the Lyapunov function value can be evaluated as follows:

$$\begin{aligned} V(x(t)) = V(x(t_0)) + \int_{t_0}^{t} \frac{\partial V(x(\tau))}{\partial t}\, d\tau = V(x(t_0)) + \int_{t_0}^{t} \frac{\partial V(x(\tau))}{\partial x} \dot{x}(\tau)\, d\tau \\ \leq \rho_{e,1} + M_f \max\{\Delta, t_{z1}\} \alpha_4(\alpha_1^{-1}(\rho_{\max})) \end{aligned} \tag{46}$$

for all $t \in [t_0, \max\{\Delta, t_{z1}\})$, where the latter inequality follows from Eq. 2, Eq. 5, and $x(t_0) \in \Omega_{\rho_{e,1}} \subset \Omega_{\rho_{1,1}} \subset \Omega_{\rho_{\max}}$. If $\rho_{e,1}$ is defined as in Eq. 40, then $V(x(t)) \leq \rho_{\max}$, $\forall t \in [t_0, \max\{\Delta, t_{z1}\})$, so that $x(t) \in \Omega_{\rho_{\max}}$ for all $t \in [t_0, \max\{\Delta, t_{z1}\})$.

Part 3. We now consider the case that $t \geq \max\{\Delta, t_{z1}\}$ and the process is not experiencing a cyberattack (i.e., $|z_j(t_k) - x(t_k)| \leq \max(e^*_{mj})$, for all $j = 1, \ldots, M$). In this case, either $z_1(t_k) \in \Omega_{\rho_{e,1}}$ so that the constraint of Eq. 8f is activated, or $z_1(t_k) \in \Omega_\rho / \Omega_{\rho_{e,1}}$ so that the constraint of Eq. 8g is activated. Consider first the case that $z_1(t_k) \in \Omega_{\rho_{e,1}}$. Eq. 8f ensures that $\tilde{x}(t)$ is maintained within $\Omega_{\rho_{e,1}}$ throughout the prediction horizon, so we must demonstrate that $x(t) \in \Omega_{\rho_{\max}}$ and $z_1(t) \in \Omega_\rho$ for $t \in [t_k, t_{k+1})$. From Proposition 1, we have the following:

$$|\tilde{x}(t) - x(t)| \leq f_W(|z_1(t_k) - x(t_k)|, \Delta) \leq f_W(\epsilon^*_M, \Delta) \tag{47}$$

for $t \in [t_k, t_{k+1})$, where the last inequality follows from Assumption 2 (i.e., when $t \geq \max\{\Delta, t_{z1}\}$ and before an attack, $|z_1(t_k) - x(t_k)| \leq e^*_{m1} \leq \epsilon^*_M$). From Proposition 2:

$$V(x(t)) \leq V(\tilde{x}(t)) + f_V(|\tilde{x}(t) - x(t)|) \leq \rho_{e,1} + f_V(f_W(\epsilon^*_M, \Delta)) \tag{48}$$

for $t \in [t_k, t_{k+1})$, where the second inequality follows from Eq. 8f and Eq. 47. If Eq. 40 holds, then if $\tilde{x}$ is maintained in $\Omega_{\rho_{e,1}}$, the actual state $x(t)$ is ensured to be inside $\Omega_{\rho_{\max}}$ for $t \in [t_k, t_{k+1})$. To ensure that the estimate for $t \in [t_k, t_{k+1})$ is also within Ω_ρ, Eq. 48 and Proposition 2 give:

$$V(z_1(t)) \leq V(x(t)) + f_V(|x(t) - z_1(t)|) \leq \rho_{e,1} + f_V(f_W(\epsilon^*_M, \Delta)) + f_V(\epsilon^*_M) \tag{49}$$

for $t \in [t_k, t_{k+1})$. When Eq. 41 holds, Eq. 49 gives that $z_1(t) \in \Omega_\rho$ for $t \in [t_k, t_{k+1})$. Therefore, when $z_1(t_k) \in \Omega_{\rho_{e,1}}$, $x(t)$ is maintained within $\Omega_{\rho_{\max}}$ and $z_1(t)$ is maintained in Ω_ρ for $t \in [t_k, t_{k+1})$ if the conditions of Theorem 3 hold.

Next, we evaluate the case that $z_1(t_k) \in \Omega_\rho/\Omega_{\rho_{e,1}}$ (i.e., Eq. 8g is activated). Considering Eqs. 8g, 2, and 4b, the bound on w, and adding and subtracting the term $\frac{\partial V(\tilde{x}(t_k))}{\partial x} f(\tilde{x}(t_k), u(t_k), 0)$ to/from $\dot{V}(x(t)) = \frac{\partial V(x(t))}{\partial x} f(x(t), u(t_k), w(t))$ and using the triangle inequality, we obtain:

$$\dot{V}(x(t)) \leq -\alpha_3(|\tilde{x}(t_k)|) + L'_x|x(t) - \tilde{x}(t_k)| + L'_w\theta_w \tag{50}$$

for all $x \in \Omega_\rho$. From $|x(t) - \tilde{x}(t_k)| \leq |x(t) - x(t_k)| + |x(t_k) - \tilde{x}(t_k)|$, we obtain that:

$$|x(t) - \tilde{x}(t_k)| \leq |x(t) - x(t_k)| + \epsilon^*_M \tag{51}$$

From Eqs. 5, 51, and 50:

$$\dot{V}(x(t)) \leq -\alpha_3(\alpha_2^{-1}(\rho_{s,1})) + L'_x(M_f\Delta + \epsilon^*_M) + L'_w\theta_w \tag{52}$$

for all $\tilde{x} \in \Omega_\rho/\Omega_{\rho_{s,1}}$. If the condition of Eq. 42 is satisfied, Eq. 52 gives:

$$V(x(t)) \leq V(x(t_k)) - \frac{\epsilon_{W,1}(t - t_k)}{\Delta},\ t\ \in [t_k, t_{k+1}) \tag{53}$$

Thus, when $z_1(t_k) \in \Omega_\rho/\Omega_{\rho_{e,1}}$, if $x(t_k) \in \Omega_{\rho_{\max}}/\Omega_{\rho_{s,1}}$, $x(t_{k+1}) \in \Omega_{\rho_{\max}}$. If instead $x(t_k) \in \Omega_{\rho_{s,1}}$, Eq. 43 guarantees that $x(t) \in \Omega_{\rho_{\min,1}} \subset \Omega_{\rho_{\max}}$ for $t \in [t_k, t_{k+1})$. From Eq. 49, $V(z_1(t)) \leq V(x(t)) + f_V(\epsilon^*_M)$. When $x(t) \in \Omega_{\rho_{\max}}$, this gives that $V(z_1(t)) \leq \rho$ if Eq. 45 holds. Applying this recursively indicates that the closed-loop state is contained within $\Omega_{\rho_{\max}}$ for all times and that the closed-loop state estimate is inside Ω_ρ when $t \geq \max\{\Delta, t_{z1}\}$.

Part 4. Finally, we consider the case that at some $t \geq \max\{\Delta, t_q\}$, the process is under a false sensor measurement cyberattack, but it is not detected by the proposed approach (i.e., $|z_i(t_k) - z_j(t_k)| \leq \epsilon_{max}$ for all $i = 1, \ldots, M$ and $j = 1, \ldots, M$). Since $|z_1(t_k) - x(t_k)| \leq \epsilon^*_M$ and the state estimate is inside Ω_ρ by the implementation strategy, boundedness of the closed-loop state in $\Omega_{\rho_{\max}}$ and state estimate in Ω_ρ are again ensured by Part 3. □

Remark 11. Although, the detection conditions have been derived for $|z_i(t_k) - z_j(t_k)|$, $i = 1, \ldots, M$ and $j = 1, \ldots, M$, if full state feedback is available, it is possible that one of the redundant estimators could be replaced by full state feedback (and/or that the resulting full state feedback could be used in place of z_1 in the output feedback LEMPC of Eq. 8). When this is done, the results of this section would continue to hold. Specifically, following similar steps to those in Section "Cyberattack-Resilient Output Feedback LEMPC: Formulation," we obtain that:

$$|\tilde{x}(t_k) - z_j(t_k)| \leq |x(t_k) + \theta_v' - z_j(t_k)| \leq |x(t_k) - z_j(t_k)| + \theta_v' \tag{54}$$

for $j = 2, \ldots, M$ (if the full state measurement takes the place of z_1). Defining $\epsilon_{\max}$ for this case as $\max[\max\{e_{mj}^*\} + \theta_v', \max\{e_{mj}^* + e_{mi}^*\}]$, $i = 2, \ldots, M$ and $j = 2, \ldots, M$ allows the control-theoretic guarantees of Theorem 3 to hold with this modified $\epsilon_{\max}$.

Remark 12. Ultimate boundedness of the closed-loop state of Eq. 1 within $\Omega_{\rho_{\min,1}}$ can also be achieved under the LEMPC of Eq. 8 even in the presence of an attack by Part 3 of the proof of Theorem 3 if the constraint of Eq. 8g begins to be always enforced after a certain time (whereas this would not be guaranteed in the presence of an attack in Detection Strategies 1 and 2). This is because not all sensors can be attacked for Detection Strategy 3, so that they effectively act like a check of one another to prevent a significant enough deviation of the actual state from the estimate (i.e., that would prevent stability goals from being achieved) from occurring without detection. The value of $\rho_{\min,1}$, however, is impacted by the size of $\rho_{e,1}$ (specifically, it must be less than $\rho_{e,1}$), which is impacted by ϵ_M^* according to the conditions of Theorem 3, so that if the value of ϵ_M^* becomes too large (allowing attacks that cause z_i, $i = 1, \ldots, M$ to deviate more significantly from x to be allowed), it may become more difficult to find a value of $\rho_{\min,1}$ that meets the conditions of Theorem 3.

Remark 13. To determine the number of sensors (and which) that could be attacked while closed-loop stability is still guaranteed under the implementation strategy until the attack is detected, it first must be determined what redundant estimators will be used, and then different scenarios with different sensors that could be attacked to cause at least one estimator to not be impacted could be developed.

Cyberattack-Resilient Output Feedback LEMPC: Chemical Process Example

In this section, a chemical process example is used to illustrate Detection Strategy 3. As in Section "Randomized LEMPC Changes to Probe for Cyberattacks: Chemical Process Example," we use a nonlinear process model of a CSTR that follows the process dynamics of Eqs. 32-33. The process states are the reactant concentration of species A (C_A) and temperature in the reactor (T). The manipulated input is the reactant feed concentration (C_{A0}). The values of the parameters of the CSTR model are taken from.[27] The vectors of deviation variables for the states and input from their steady-state values, $C_{As} = 2$ kmol/m^3, $T_s = 350$ K, $C_{A0s} = 4.0$ kmol/m^3, respectively, are $x = [x_1 \ x_2]^T = [C_A - C_{As} \ T - T_s]^T$ and $u = C_{A0} - C_{A0s}$. The process model represented by Eqs. 32-33 is numerically integrated using the explicit Euler method with integration step of 10^{-3} h. The economic stage cost $L_e = k_0 e^{-E/(RT)} C_A^2$ was utilized for this proposed control/detection scheme.

Lyapunov-based stability constraints in Eqs. 8f-8g were designed using a quadratic Lyapunov function $V = x^T P x$, where $P = [110.11 \ 0; 0 \ 0.12]$. The Lyapunov-based controller utilized was a proportional controller of the form $h(x) = -1.6x_1 - 0.01x_2$ ([27]) subject to input constraints ($|u| \leq 3.5$ kmol/m^3). The stability region was set to $\rho = 440$ (i.e., $\Omega_\rho = \{x \in R^2 : V(x) \leq \rho\}$) and $\rho_e = 330$. The LEMPC receives full state feedback (Remark 11) with the full system state $x = [x_1 \ x_2]^T$ which is measured and sent to the LEMPC at synchronous time instants t_k. A high-gain observer is used as the redundant estimator to estimate the reactant concentration of species A from continuously available temperature measurements (x_2). The design of this high-gain observer follows[27] with respect to a transformed system state obtained via input-output linearization. The observer equation using the set of new coordinates is as follows:

$$\dot{\hat{z}} = A\hat{z} + L(y - C\hat{z}) \tag{55}$$

where $\hat{z}$ is the state estimate vector in the new coordinate, y is the output measurement, $A = [0 \ 1; 0 \ 0]$, $C = [1 \ 0]$, and $L = [100 \ 10000]^T$. To obtain the state estimate of the system z, the inverse transformation $T^{-1}(\hat{z})$ is applied.

For the detection conditions of Eq. 36, data from an attack-free scenario is gathered by simulating the process under the proposed LEMPC described above. We simulate this attack-free event over 1 h of operation with the system state initialized off steady-state at $x_{init} = [C_A - C_{As} \ T - T_s][-0.7$ kmol/m^3 -30 K$]^T$ in MATLAB R2017b, with the function tolerance set to 10^{-7}. A constraint of the form of Eq. 8f was enforced at the end of each sampling period both when the constraint of Eq. 8g was activated and when it was not. The controller receives a state measurement subject to bounded measurement noise and the process is subject to bounded disturbances. Specifically, the noise is represented by a standard normal distribution with mean zero, standard deviations of 0.01 kmol/m^3 and 0.5 K, and bounds of 0.02 kmol/m^3 and 0.5 K for the concentration of the reactant and reactor temperature, respectively. In addition, process disturbances was added to the right-hand side of the differential equations describing the rates of change of C_A and T with zero mean and standard deviations of 0.5 kmol/m^3 h and 2 K/h, and bounds of 2 kmol/m^3 h and 5 K/h, respectively. The norm $|\tilde{x}(t_k) - z(t_k)|$ was bounded after 0.2 h under an attack-free simulation below 0.9520 (which was taken to be $\epsilon_{\max}$ and used to flag attacks in the remainder of the example).

To ensure that not all estimators are impacted by attacks as required, the control system under state feedback LEMPC is subjected to false state measurements of reactant concentration (which have the form $x_1 + 0.1$ kmol/m^3 h; i.e., the temperature measurements are intact and only the full state feedback measurements are impacted with the high gain observer not impacted as it only uses measurements of the un-attacked sensor, the temperature). These false measurements are always provided to the controller after 0.3 h of operation. We simulate the process under the proposed control design over 1 h of operation with the process state initialized off steady-state again from $x_{init} = [-0.7$ kmol/m^3 -30 K$]^T$ in MATLAB R2017b using fmincon. The measurement noise and disturbances follow the same standard normal distribution described above. To solve the optimization problem of Eq. 8, we use the following initial guess: at the first sampling time the value of the Lyapunov-based controller $h(x)$ is used while for the subsequent sampling times, a shifted version of the optimal solution of the previous sampling time is utilized and the guess of the last entry of the optimal input vector is based on $h(x)$. Fig. 2 depicts the closed-loop state trajectory in contrast with the closed-loop state estimate trajectory after 0.2 h of operation. As soon as the cyberattack policy was implemented at 0.3 h, the control/detection strategy promptly flagged abnormal behavior at the subsequent sampling time, when the closed-loop state was still within the stability region, which could allow a backup policy to be employed.

We can also explore a case where an attack happens but the proposed detection mechanism does not flag it during process operation. Specifically, we consider that the false state measurements for

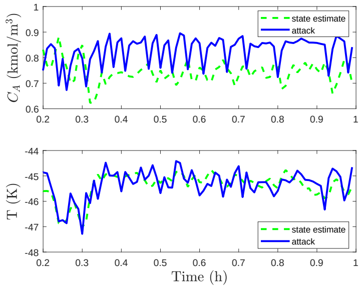

Figure 2: Comparison between the closed-loop state trajectory under attack (solid line) and the closed-loop state estimate trajectory (dashed lines) after 0.2 h of operation under the state feedback LEMPC.

reactant concentration above now have the form $x_1 + 0.01$ kmol/m^3 h (which follows an attack trajectory with similarities to that in Fig. 2 but a better match between the measurement and estimate trajectories for C_A) and are always provided to the controller after 0.3 h of operation. In this case, although the attack was not flagged during the simulation, the closed-loop state was maintained in Ω_ρ under the proposed control design for the time period simulated, demonstrating the concept that with the process subject to sufficiently small measurement noise and disturbances, the closed-loop state can be maintained in Ω_ρ.

The proposed control/detection approach may also identify an attack if both state measurements are attacked as long as the condition $|\tilde{x}(t_k) - z(t_k)| \leq \epsilon_{\max}$ to flag an attack still holds (despite that attack detection if all measurements are attacked is not guaranteed in Section "Cyberattack-Resilient Output Feedback LEMPC: Stability and Feasibility Analysis" to be flagged). To show this, we consider the case where false state measurements of both reactant concentration and temperature of the form $x_1 + 0.01$ kmol/m^3 and $x_2 + 1$ K, respectively, are provided to the sensors after 0.3 h. As soon as this attack was implemented (at 0.3 h), an attack was detected since the norm $|\tilde{x}(t_k) - z(t_k)|$ was larger than the threshold (again with the closed-loop state still in the stability region at the detection time).

Conclusions

In light of the difficulty of guaranteeing cyberattack-resilience using LEMPC design only, as was analyzed in our prior work,[14] this work aimed to investigate how the control-theoretic guarantees of LEMPC might be leveraged with detection techniques to attempt to prevent false sensor measurements from causing closed-loop stability issues in a chemical plant. Three cyberattack detection concepts using LEMPC design were explored. The first strategy focused on the use of random designs of LEMPC's around alternative steady-states within the stability region to check whether the theoretical property of the randomly generated LEMPC's (i.e., that the value of the Lyapunov function that the LEMPC is designed with respect to should decrease over the sampling period following the activation of this LEMPC) is met by the process state measurements. The second strategy focused on a state prediction, detection, and control framework that guarantees that the closed-loop state is maintained in a stability region for one sampling period after an undetected attack. Finally, the third strategy focused on a state estimation, detection, and control framework that assumed that multiple state estimators were available for the process and that at least one could be compromised by a false sensor measurement attack. A key challenge for future work is better understanding the limits of what can be achieved, theoretically and fundamentally, in terms of securing control systems against cyberattacks on their various components. This work focused only on sensor attacks; however, there are many possible routes by which an attack may be performed on a cyberphysical system, and when the attacks are too extensive (e.g., the attacker gains control of many aspects of the control loop) it may be difficult to provide guarantees on process behavior during the attack.

1. Acknowledgements

Financial support from the National Science Foundation CNS-1932026, Air Force Office of Scientific Research under award number FA9550-19-1-0059, and Wayne State University is gratefully acknowledged.

Literature Cited

[1] N. Tuptuk, S. Hailes, Security of smart manufacturing systems, Journal of Manufacturing Systems 47 (2018) 93–106.

[2] D. J. Mahoney, T. C. ed., Cybersecurity for manufacturers: Securing the digitized and con-

nected factory, Report No. MF-TR-2017-0202, MForesight: Alliance for Manufacturing Foresight and Computing Research Association's Computing Community Consortium.

[3] Z. Wu, F. Albalawi, J. Zhang, Z. Zhang, H. Durand, P. D. Christofides, Detecting and handling cyber-attacks in model predictive control of chemical processes, Mathematics 6 (2018) 22 pages.

[4] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, S. Sastry, Attacks against process control systems: Risk assessment, detection, and response, in: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, Association for Computing Machinery, New York, NY, USA, 2011, p. 355–366.

[5] S. E. Chandy, A. Rasekh, Z. A. Barker, M. E. Shafiee, Cyberattack detection using deep generative models with variational inference, Journal of Water Resources Planning and Management 145 (2) (2019) 04018093.

[6] H. Karimipour, A. Dehghantanha, R. M. Parizi, K.-K. R. Choo, H. Leung, A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids, IEEE Access 7 (2019) 80778–80788.

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

[8] S. J. Qin, T. A. Badgwell, A survey of industrial model predictive control technology, Control Engineering Practice 11 (2003) 733–764.

[9] R. Ma, S. Basumallik, S. Eftekharnejad, F. Kong, Recovery-based model predictive control for cascade mitigation under cyber-physical attacks, in: 2020 IEEE Texas Power and Energy Conference (TPEC), IEEE, 2020, pp. 1–6.

[10] Q. Sun, K. Zhang, Y. Shi, Resilient model predictive control of cyber–physical systems under dos attacks, IEEE Transactions on Industrial Informatics 16 (7) (2019) 4920–4927.

[11] S. Liu, Y. Song, G. Wei, X. Huang, RMPC-based security problem for polytopic uncertain system subject to deception attacks and persistent disturbances, IET Control Theory & Applications 11 (10) (2017) 1611–1618.

[12] G. Franzè, F. Tedesco, W. Lucia, Resilient control for cyber-physical systems subject to replay attacks, IEEE Control Systems Letters 3 (4) (2019) 984–989.

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

[14] H. Durand, A nonlinear systems framework for cyberattack prevention for chemical process control systems, Mathematics 6 (2018) 44 pages.

[15] M. Ellis, H. Durand, P. D. Christofides, A tutorial review of economic model predictive control methods, Journal of Process Control 24 (2014) 1156–1178.

[16] J. B. Rawlings, D. Angeli, C. N. Bates, Fundamentals of economic model predictive control, in: Proceedings of the IEEE Conference on Decision and Control, Maui, Hawaii, 2012, pp. 3851–3861.

[17] H. Durand, M. Wegener, Mitigating safety concerns and profit/production losses for chemical process control systems under cyberattacks via design/control methods, Mathematics 8 (4).

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

[19] H. Oyama, H. Durand, Control system cyberattack detection using lyapunov-based economic model predictive control, 2020 IFAC World Congress, 2020.

[20] H. Durand, M. Wegener, Mitigating cyberattack impacts using lyapunov-based economic model predictive control, Proceedings of the American Control Conference.

[21] M. Ellis, J. Zhang, J. Liu, P. D. Christofides, Robust moving horizon estimation based output feedback economic model predictive control, Systems & Control Letters 68 (2014) 101–109.

[22] L. Lao, M. Ellis, H. Durand, P. D. Christofides, Real-time preventive sensor maintenance using robust moving horizon estimation and economic model predictive control, AIChE Journal 61 (2015) 3374–3389.

[23] J. H. Ahrens, H. K. Khalil, High-gain observers in the presence of measurement noise: A switched-gain approach, Automatica 45 (4) (2009) 936–943.

[24] D. M. de la Peña, P. D. Christofides, Lyapunov-based model predictive control of nonlinear systems subject to data losses, IEEE Transactions on Automatic Control 53 (9) (2008) 2076–2089.

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

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

[27] M. Heidarinejad, J. Liu, P. D. Christofides, State-estimation-based economic model predictive control of nonlinear systems, Systems & Control Letters 61 (9) (2012) 926–935.

List of Figures

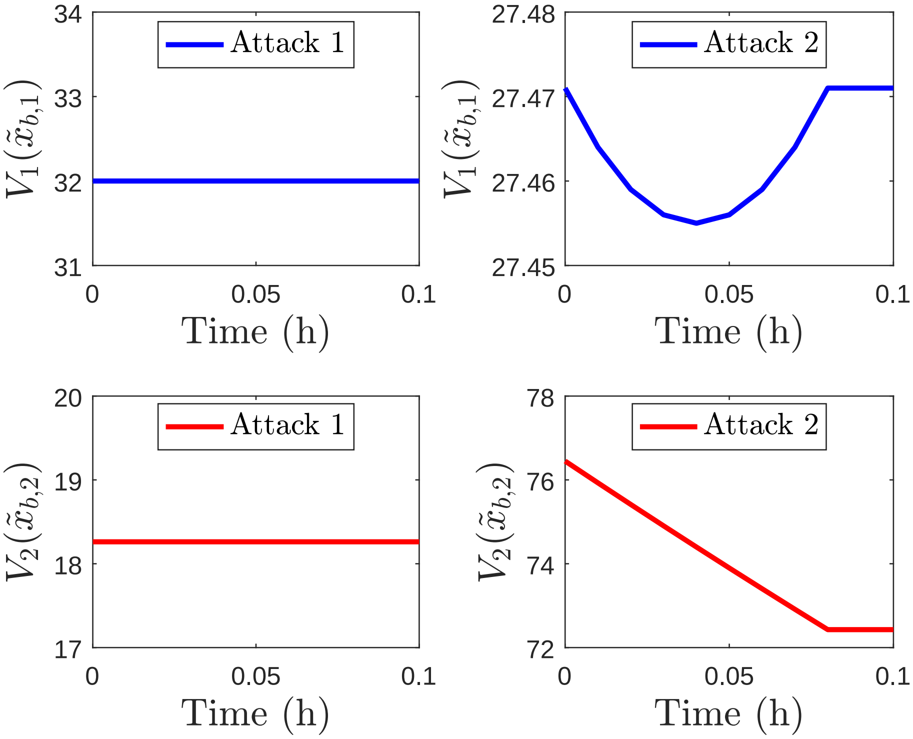

Figure 3: V_1 (top plots) and V_2 (bottom plots) profiles over 0.1 h of operation for the process example in the presence of different cyberattack policies.

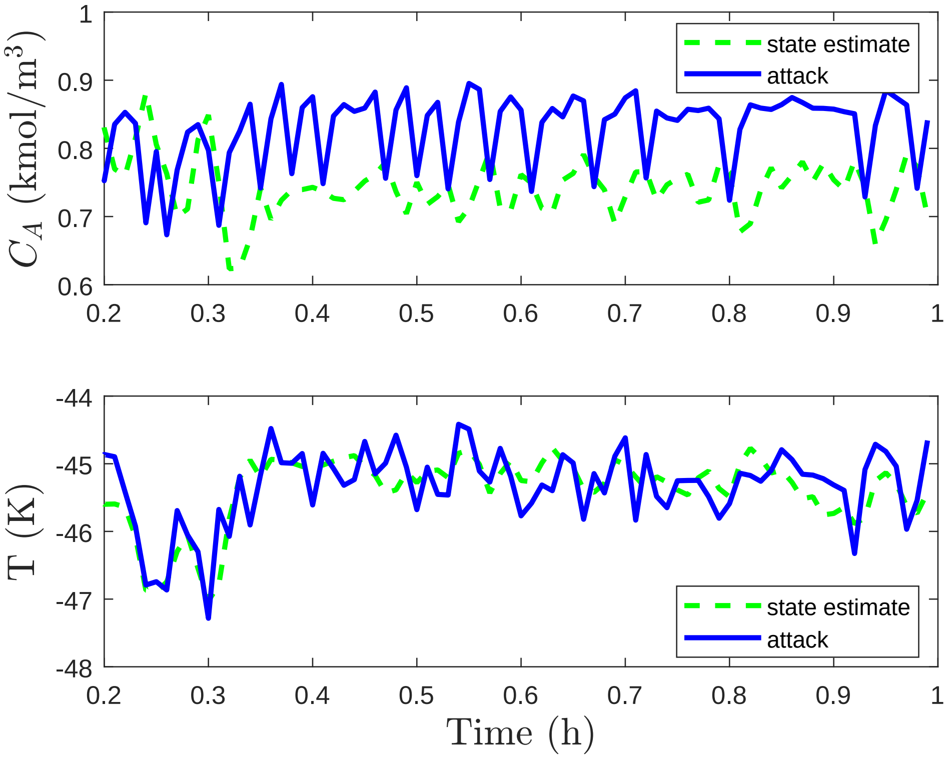

Figure 4: Comparison between the closed-loop state trajectory under attack (solid line) and the closed-loop state estimate trajectory (dashed lines) after 0.2 h of operation under the state feedback LEMPC.