Mitigating Cyberattack Impacts Using Lyapunov-Based Economic Model Predictive Control

Helen Durand[1] and Matthew Wegener[1]

***Abstract*— One of the pressing concerns for next-generation manufacturing is the development of techniques for guaranteeing that a control system is cyberattack-resilient in the sense that even if a cyberattack is successful at breaking information technology-based defenses (e.g., it succeeds at providing a false sensor measurement to the controller), closed-loop stability is still maintained. Our prior work has provided a nonlinear systems definition for cyberattacks. This work explores how a nonlinear systems perspective on cyberattack-resilience for false sensor measurements provided to controllers may allow an economic model predictive control (EMPC) formulation known as Lyapunov-based EMPC (LEMPC) to be designed such that if a cyberattack occurs at a sampling time, the closed-loop state will not leave a region where a known feedback control law exists that can stabilize the origin of the closed-loop system if the cyberattack is detected and non-falsified state measurements are then provided within that sampling period.**

I. INTRODUCTION

Cyberattacks on industrial control systems are becoming a more significant concern to safe and continuous operation of chemical processes. Demonstrated with the Stuxnet attack on Programmable Logic Controllers (PLCs) at the Natanz uranium enrichment plant in 2010 [1], cyberattacks have the ability to disrupt, damage, and destroy national infrastructure and commercial production facilities. If the proper product and process quantities are not adequately checked (e.g., impurities in products which can cause issues with their end use, as in, for example, the pharmaceutical industry) via effective quality control, issues could arise both during manufacturing and use of products. For many chemical-based processes, quality control is in place, as are many safeguards for preventing unexpected scenarios from causing plant accidents. However, attacks could still significantly impact production levels, which can pose national security issues for products that are needed to keep industries and daily life running, such as the chemical and refining industries, or the pharmaceutical industry. This indicates the need for developing additional cyberattack-resilient control designs. An important direction for cyberattack-resilient control frameworks is integrating control, state estimation, and attack detection to maintain closed-loop stability [2]. For example, [3] places bounds on the minimum number of sensors that could be provided with false measurements while still allowing reasonable state estimates for a linear system to be obtained for use in place of feedback to the control systems. Various attack detection methods have also been developed, including a method based on neural networks [4] and a method based on clustering [5].

These prior works imply that a combined detection, state estimation, and response strategy may be beneficial for maintaining closed-loop stability and close-to-normal production levels for nonlinear systems operated continuously under an optimization-based controller known as economic model predictive control (EMPC) [6], [7], [8] even in the presence of cyberattacks involving false state measurements provided to the control systems. A first step in working toward the development of such an integrated strategy is to better understand the detection-control interface, and how an EMPC could be designed to ensure that the closed-loop state does not exit a region of state-space from which closed-loop stability can be maintained with non-falsified measurements within a sampling period after the attack occurs. This work focuses on this task in the context of a specific EMPC design known as Lyapunov-based EMPC (LEMPC) [9]. We make precise connections between handling measurement noise and disturbances and handling cyberattacks in the context of the proposed design.

II. PRELIMINARIES

A. Notation

Consider the following notation where the Euclidean norm of a vector is given by $|\cdot|$, a class $\mathcal{K}$ function is a function $\alpha : [0, a) \to [0, \infty)$ where $\alpha(0) = 0$ and the function strictly increases, x^T signifies the transpose of the vector x, and "/" represents set subtraction so that $x \in A/B := \{x \in R^n : x \in A, x \notin B\}$. $\Omega_\rho := \{x \in R^n : V(x) \leq \rho\}$ denotes the level set of a positive definite function V.

B. Class of Systems

The class of systems considered is the following:

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

$$y(t) = x(t) + v(t) \tag{2}$$

where $x \in R^n$ represents the vector of bounded process states, $u \in U \subset R^m$ represents the vector of bounded manipulated inputs, and $w \in W \subset R^l$ represents a vector of bounded disturbances (i.e., $W := \{w \in R^l : |w| \leq \theta\}$). $y \in R^n$ is an output measurement vector introduced to reflect that bounded measurement noise (with noise vector $v \in R^n$; i.e., $v \in V := \{v \in R^n : |v| \leq \phi\}$) is considered. f is a locally Lipschitz nonlinear vector function with $f(0, 0, 0) = 0$. We consider that there exists a sufficiently smooth positive definite Lyapunov function $V : R^n \to R_+$,

[1] Helen Durand and Matthew Wegener are with Department of Chemical Engineering and Materials Science, Wayne State University, 5050 Anthony Wayne Drive, Detroit, MI helen.durand@wayne.edu

class $\mathcal{K}$ functions $\alpha_j(\cdot)$, $j = 1, \ldots, 4$, and a controller $h_1(x)$ that can asymptotically stabilize the origin of the nominal ($w(t) \equiv 0$) closed-loop system of Eq. 1 such that:

$$\alpha_1(|x|) \leq V(x) \leq \alpha_2(|x|) \tag{3}$$

$$\frac{\partial V(x)}{\partial x} f(x, h_1(x), 0) \leq -\alpha_3(|x|) \tag{4}$$

$$\left| \frac{\partial V(x)}{\partial x} \right| \leq \alpha_4(|x|) \tag{5}$$

$$h_1(x) \in U \tag{6}$$

$\forall\ x \in D \subset R^n$, where D is an open neighborhood of the origin. The level set $\Omega_\rho \subset D \cap X$ of V is the "stability region." It is assumed that $h_1(x)$ satisfies:

$$|h_{1,i}(x) - h_{1,i}(\hat{x})| \leq L_h |x - \hat{x}| \tag{7}$$

for all $x, \hat{x} \in \Omega_\rho$, with $L_h > 0$, where $h_{1,i}$ represents the i-th component of h_1. Also, we consider that:

$$|f(x, u, w)| \leq M \tag{8}$$

$$|f(x_1, u_1, w) - f(x_1, u_2, w)| \leq L_u |u_1 - u_2| \tag{9}$$

$$|f(x_1, u_1, w) - f(x_2, u_1, 0)| \leq L_x |x_1 - x_2| + L_w |w| \tag{10}$$

$$\begin{aligned} \left| \frac{\partial V(x_1)}{\partial x} f(x_1, u_1, w) - \frac{\partial V(x_2)}{\partial x} f(x_2, u_1, 0) \right| &\leq L'_x |x_1 - x_2| \\ &+ L'_w |w| \end{aligned} \tag{11}$$

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

C. Lyapunov-based Economic Model Predictive Control

LEMPC [9] is defined by:

$$\begin{aligned} \min_{u(t) \in S(\Delta)} \quad & \int_{t_k}^{t_{k+N}} L_e(\tilde{x}(\tau), u(\tau))\, d\tau & \text{(12a)} \\ \text{s.t.} \quad & \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0) & \text{(12b)} \\ & \tilde{x}(t_k) = x(t_k) & \text{(12c)} \\ & \tilde{x}(t) \in X,\ \forall\, t \in [t_k, t_{k+N}) & \text{(12d)} \\ & u(t) \in U,\ \forall\, t \in [t_k, t_{k+N}) & \text{(12e)} \\ & V(\tilde{x}(t)) \leq \rho_e,\ \ \forall\, t \in [t_k, t_{k+N}), & \\ & \qquad \text{if } x(t_k)\ \in\ \Omega_{\rho_e} & \text{(12f)} \\ & \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0) & \\ & \quad \leq \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), h_1(x(t_k)), 0) & \\ & \text{if }\ x(t_k) \in \Omega_\rho / \Omega_{\rho_e} & \text{(12g)} \end{aligned}$$

where the notation $u(t) \in S(\Delta)$ signifies 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 stage cost L_e in Eq. 12 may reflect the process economics, and its time integral is evaluated throughout the prediction horizon with predictions $\tilde{x}$ of the process state obtained from Eq. 12b (which represents the model of Eq. 1, but with $w(t) \equiv 0$, which is termed the "nominal" model). Eq. 12b is initialized from the measured state $x(t_k)$ at t_k via Eq. 12c. Eqs. 12d-12e represent state and input constraints. LEMPC is applied in a receding horizon fashion, and the optimal solution at t_k is denoted by $u^*(t_i|t_k)$, where $i = k, \ldots, k+N-1$. $\Omega_{\rho_e} \subset \Omega_\rho$ is a level set of V which renders Ω_ρ forward invariant under the LEMPC of Eq. 12.

III. LEMPC for Cyberattack Mitigation

An attack on an LEMPC could involve a false state measurement being provided; this can be considered a form of measurement noise. However, it does not necessarily meet the bound assumed on v above; in other words, a process may exhibit both measurement noise and disturbances (as considered in Eqs. 1-2 above), in the presence of which the controller may be designed to still stabilize the origin, but may not be designed to handle cyberattacks. This section makes precise connections between false sensor measurement cyberattacks and measurement noise theoretically, beginning with an LEMPC scheme (using constraints called "input rate of change" constraints from [11]) to be considered for stabilizing the closed-loop system of Eq. 1 in both the measurement noise and false sensor measurement cases. We will analyze the conditions under which it is stabilizing in the presence of measurement noise, and then discuss how the measurement noise analysis might be extended to the cyberattack case, and also differentiated from it.

A. LEMPC Formulation

We consider the LEMPC formulation from [11], but accounting for measurement noise, as follows:

$$\begin{aligned} \min_{u(t) \in S(\Delta)} \quad & \int_{t_k}^{t_{k+N}} L_e(\tilde{x}(\tau), u(\tau))\, d\tau & \text{(13a)} \\ \text{s.t.} \quad & \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t), 0) & \text{(13b)} \\ & \tilde{x}(t_k) = x(t_k) & \text{(13c)} \\ & \tilde{x}(t) \in X,\ \forall\, t \in [t_k, t_{k+N}) & \text{(13d)} \\ & u(t) \in U,\ \forall\, t \in [t_k, t_{k+N}) & \text{(13e)} \\ & |u_i(t_k) - h_{1,i}(\tilde{x}(t_k))| \leq \epsilon_r,\ i = 1, \ldots, m & \\ & & \text{(13f)} \\ & |u_i(t_j) - h_{1,i}(\tilde{x}(t_j))| \leq \epsilon_r,\ i = 1, \ldots, m, & \\ & \qquad j = k+1, \ldots, k+N-1 & \text{(13g)} \\ & V(\tilde{x}(t)) \leq \rho'_e,\ \ \forall\, t \in [t_k, t_{k+N}), & \\ & \qquad \text{if } x(t_k)\ \in\ \Omega_{\rho'_e} & \text{(13h)} \\ & \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), u(t_k), 0) & \\ & \quad \leq \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), h_1(x(t_k)), 0) & \\ & \text{if }\ x(t_k) \in \Omega_\rho / \Omega_{\rho'_e} & \text{(13i)} \end{aligned}$$

Compared to the level sets in Eq. 12, ρ_e is replaced by ρ'_e, where $\rho'_e < \rho_e$, $\rho' < \rho$, and $\Omega_{\rho'_e} \subset \Omega_{\rho'}$. These regions are selected to guarantee closed-loop stability even in the presence of measurement noise, where that noise may be bounded by ϕ like v, or has the potential to be larger than ϕ in a cyberattack. The conditions on ρ'_e and ρ' which allow closed-loop stability to be guaranteed with this design in both cases are presented in the subsequent section.

B. Stability and Feasibility Analysis: Measurement Noise Case

To make precise connections between the cyberattack and measurement noise cases for the LEMPC of Eq. 13, we begin by providing the conditions under which closed-loop stability is maintained for this LEMPC in the presence of measurement noise. To develop these conditions, we introduce the following definition.

Definition 1: Consider the state trajectories from $t \in [t_0, t_1)$ that are the solutions of the systems

$$\dot{x}_a = f(x_a(t), u^*(x_0), w(t)) \tag{14}$$

$$\dot{x}_b = f(x_b(t), u^*(x_0 + \delta), w(t)) \tag{15}$$

where $x_a(t_0) = x_b(t_0) = x_0$, and $u^*(x_0)$ is the optimal input for $t \in [t_0, t_1)$ computed from the LEMPC of Eq. 13 with when a fully accurate state measurement $\tilde{x}_a(t_0) = x_0$ is provided to the LEMPC, while $u^*(x_0 + \delta)$ is the optimal input for $t \in [t_0, t_1)$ when the LEMPC receives a noisy measurement $\tilde{x}_b(t_0) = x_0 + \delta$ ($|\delta| \leq \phi$). Thus, $x_a(t)$, $t \in [t_0, t_1)$, represents the behavior of the process of Eq. 1 under the input computed in the case of perfect state measurement sampling from t_0 to t_1, and $x_b(t)$, $t \in [t_0, t_1)$, represents the behavior of the process from t_0 to t_1 under the input computed when measurement noise is present at t_0.

Because the input rate of change constraints are used, the m components $u_i^*(x_0)$ and $u_i^*(x_0 + \delta)$, $i = 1, \dots, m$, of $u^*(x_0)$ and $u^*(x_0 + \delta)$ satisfy:

$$|u_i^*(x_0) - h_{1,i}(\tilde{x}_a(t_0))| \leq \epsilon_r \tag{16}$$

$$|u_i^*(x_0 + \delta) - h_{1,i}(\tilde{x}_b(t_0))| \leq \epsilon_r \tag{17}$$

Furthermore, the input rate of change constraints result in the proposition below, which bounds $|x_a - x_b|$.

Proposition 1: Consider the systems in Definition 1. The following bound holds for $x_a(t), x_b(t) \in \Omega_\rho$:

$$|x_a(t) - x_b(t)| \leq f_u(t) \tag{18}$$

for $t \in [0, t_1)$, where

$$f_u(\tau) := \frac{L_u(2\epsilon_r + L_h|\delta|)\sqrt{m}}{L_x}(e^{L_x \tau} - 1) \tag{19}$$

Proof 1: The proof consists of two parts where $|u^*(x_0) - u^*(x_0 + \delta)|$ is shown to be bounded and Eq. 18 is derived.

Part 1. From Eq. 16 and Eq. 7, for all $i = 1, \dots, m$:

$$\begin{aligned} &|u_i^*(x_0) - u_i^*(x_0 + \delta)| \\ &= |u_i^*(x_0) + h_{1,i}(\tilde{x}_a(t_0)) - h_{1,i}(\tilde{x}_a(t_0)) + h_{1,i}(\tilde{x}_b(t_0)) \\ &\quad - h_{1,i}(\tilde{x}_b(t_0)) - u_i^*(x_0 + \delta)| \\ &\leq 2\epsilon_r + L_h|\tilde{x}_a(t_0) - \tilde{x}_b(t_0)| \\ &\leq 2\epsilon_r + L_h|\delta| \end{aligned} \tag{20}$$

Part 2. Consider state trajectories x_a and x_b given by Eqs. 14-15 under $u^*(x_0)$ and $u^*(x_0 + \delta)$ from t_0 to t_1:

$$x_a(t) = x_a(t_0) + \int_{t_0}^{t} f(x_a(s), u^*(x_0), w)ds \tag{21}$$

$$x_b(t) = x_b(t_0) + \int_{t_0}^{t} f(x_b(s), u^*(x_0 + \delta), w)ds \tag{22}$$

Subtracting Eq. 22 from Eq. 21, adding and subtracting $f(x_a(s), u^*(x_0 + \delta), w(s))$ on the right-hand side, taking the absolute value of both sides, and utilizing the triangle inequality gives:

$$\begin{aligned} &|x_a(t) - x_b(t)| \\ &\leq \int_0^t [|f(x_a(s), u^*(x_0), w(s)) \\ &- f(x_a(s), u^*(x_0 + \delta), w(s))| \\ &+ |f(x_a(s), u^*(x_0 + \delta), w(s)) \\ &- f(x_b(s), u^*(x_0 + \delta), w(s))|]\, ds \end{aligned} \tag{23}$$

for all $t \in [0, t_1)$. Using Eqs. 9-10 and 23:

$$\begin{aligned} &|x_a(t) - x_b(t)| \leq \int_0^t [L_u|u^*(x_0) - u^*(x_0 + \delta)| \\ &+ L_x|x_a(s) - x_b(s)|]\, ds \\ &\leq L_u(2\epsilon_r + L_h|\delta|)\sqrt{m}t + L_x \int_0^t |x_a(s) - x_b(s)|ds \end{aligned} \tag{24}$$

for all $t \in [0, t_1)$. Finally, using the Gronwall-Bellman inequality [12], Eqs. 18-19 are obtained.

We now present two propositions.

Proposition 2: [13], [9], [14] Consider the systems

$$\dot{x}_y(t) = f(x_y(t), \bar{u}(t), w(t)) \tag{25}$$

$$\dot{x}_z(t) = f(x_z(t), \bar{u}(t), 0) \tag{26}$$

with initial states $|x_y(t_0) - x_z(t_0)| \leq |\delta|$, where $x_y(t_0)$ and $x_z(t_0)$ are in Ω_ρ. There exists a $\mathcal{K}$ function $f_W(\cdot)$ such that

$$|x_y(t) - x_z(t)| \leq f_W(|\delta|, t - t_0) \tag{27}$$

for all $x_y(t), x_z(t) \in \Omega_\rho$, $u \in U$, and $w(t) \in W$ with:

$$f_W(s, \tau) = \left(s + \frac{L_w \theta}{L_x}\right) e^{L_x \tau} - \frac{L_w \theta}{L_x} \tag{28}$$

Proof 2: This proof closely follows that for Proposition 1. Starting from the representations of x_y and x_z in the integral form similar to Eqs. 21-22, subtracting one of the resulting equations from the other, adding and subtracting $f(x_y, \bar{u}, 0)$ to the right-hand side, taking the absolute value of each side, applying the triangle inequality, and using Eq. 10 and $|w| \leq \theta$, with $|x_y(t_0) - x_z(t_0)| \leq |\delta|$, we obtain:

$$|x_y - x_z| \leq |\delta| + L_w \theta t + \int_0^t L_x |x_y - x_z| \tag{29}$$

Using the Gronwall-Bellman inequality gives Eq. 28.

Proposition 3: [13], [9] Consider the Lyapunov function $V(\cdot)$ of the system of Eq. 1. There exists a quadratic function $f_V(\cdot)$ such that:

$$V(x) \leq V(\hat{x}) + f_V(|x - \hat{x}|) \tag{30}$$

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

$$f_V(s) = \alpha_4(\alpha_1^{-1}(\rho))s + M_v s^2 \tag{31}$$

where M_v is a positive constant.

The theorem below provides the conditions under which closed-loop stability is guaranteed for the LEMPC of Eq. 13 in the presence of sufficiently small bounded measurement noise and disturbances. Compared to [14], which also develops an LEMPC that can handle bounded measurement noise and disturbances, the theorem holds with input rate of change constraints and does not consider a state estimator due to the assumption that full state measurements are available (though noisy) and therefore is stated explicitly for clarity.

Theorem 1: Consider the system of Eq. 1 in closed-loop under the LEMPC design of Eq. 13 based on a controller $h_1(x)$ that satisfies the assumptions of Eqs. 3-6 and 7. Let $\epsilon_w > 0$, $\Delta > 0$, $\rho > \rho' > \rho'_e > \rho_{\min} > \rho_s > 0$, where $\rho_{samp} > \rho'_e$ is defined as the smallest level set of V that guarantees that if $V(x_b(t_k)) \in \Omega_\rho/\Omega_{\rho_{samp}}$, $V(\tilde{x}_b(t_k)) \in \Omega_\rho/\Omega_{\rho_{e'}}$, and $\rho > \rho_{samp2} > \rho_{samp}$ satisfy:

$$\rho'_e \leq \rho' - f_V(f_W(0,\Delta)) \tag{32}$$

$$-\alpha_3(\alpha_2^{-1}(\rho_s)) + L'_x M\Delta + L'_w\theta \leq -\epsilon_w/\Delta \tag{33}$$

$$\rho' + f_V(f_u(\Delta)) \leq \rho_{samp2} \tag{34}$$

$$-\alpha_3(\alpha_2^{-1}(\rho'_e)) + L'_x M\Delta + L'_x|\delta| + L'_w\theta \leq -\epsilon'_w/\Delta \tag{35}$$

$$\rho_{\min} = \max\{V(x_b(t+\Delta)) : x_b(t) \in \Omega_{\rho_s}\} \tag{36}$$

$$\rho_{samp2} \geq \max\{V(x_b(t+\Delta)) : x_b(t) \in \Omega_{\rho_{samp}}/\Omega_{\rho'_e}\} \tag{37}$$

$$\rho \geq \max\{V(\tilde{x}_b(t_k)) : V(x(t_k)) \in \Omega_{\rho_{samp2}}\} \tag{38}$$

If $x(t_0) \in \Omega_{\rho_{samp2}}$ and $N \geq 1$, then the state $x(t) \in \Omega_{\rho_{samp2}}$ for all $t \geq 0$, and the state measurement at each sampling time is in Ω_ρ, for $|\delta| = \phi$.

Proof 3: $h_1(x)$ implemented in sample-and-hold is a feasible solution to Eq. 13 from [11] when $\tilde{x}_b(0) \in \Omega_\rho$ and Eq. 33 holds. To prove the stability result, we consider four cases: Case 1) the actual process state at t_0 ($x_a(t_0) = x_b(t_0)$) is $x_0 \in \Omega_{\rho'_e}$ and the state measurement at t_0 (i.e., $\tilde{x}_b(0)$) is $x_0 + \delta \in \Omega_{\rho'_e}$; Case 2) the actual process state at t_0 is $x_0 \in \Omega_{\rho_{samp2}}/\Omega_{\rho'_e}$ and $\tilde{x}_b(0) = x_0 + \delta \in \Omega_\rho/\Omega_{\rho'_e}$; Case 3) the actual process state at t_0 is $x_0 \in \Omega_{\rho_{samp}}/\Omega_{\rho'_e}$ but $\tilde{x}_b(0) = x_0 + \delta \in \Omega_{\rho'_e}$; and Case 4) the actual process state at t_0 is $x_0 \in \Omega_{\rho'_e}$ but $\tilde{x}_b(0) = x_0 + \delta \in \Omega_\rho/\Omega_{\rho'_e}$.

Case 1. If the LEMPC receives the state measurement $x_0 \in \Omega_{\rho'_e}$, [11] shows that under the condition in Eq. 32, $V(x_a(t_1)) \leq \rho'$. From Eq. 13h, $V(\tilde{x}_b(t_1)) \leq \rho'_e$. From Propositions 1 and 3, and Eq. 19:

$$\begin{aligned} V(x_b(t_1)) &\leq V(x_a(t_1)) + f_V(|x_a(t_1) - x_b(t_1)|) \\ &\leq \rho' + f_V(f_u(\Delta)) \end{aligned} \tag{39}$$

if $V(x_b(t_1)) \in \Omega_{\rho_{samp2}}$, which follows if Eq. 34 holds.

Case 2. If the LEMPC receives the state measurement $x_0 \in \Omega_{\rho_{samp2}}/\Omega_{\rho'_e}$, [11] shows that with Eq. 33, $V(x_a(t)) \leq V(x_0)$, $\forall\ t \in [0, t_1)$. To determine whether $V(x_b(t)) \leq V(x_0)$, $\forall\ t \in [0, t_1)$, we note that from Eq. 13i and Eq. 4:

$$\frac{\partial V(\tilde{x}_b(t_0))}{\partial x} f(\tilde{x}_b(t_0), u^*(x_0+\delta), 0) \leq -\alpha_3(|\tilde{x}_b(t_0)|) \tag{40}$$

The time-derivative of V along the closed-loop state trajectories of x_b from 0 to t_1 satisfies:

$$\begin{aligned} \dot{V}(x_b(\tau)) &= \frac{\partial V(x_b(\tau))}{\partial x} f(x_b(\tau), u^*(x_0+\delta), w(\tau)) \\ &\leq -\alpha_3(|\tilde{x}_b(t_0)|) + \left| \frac{\partial V(x_b(\tau))}{\partial x} f(x_b(\tau), u^*(x_0+\delta), w(\tau)) \right. \\ &\quad \left. - \frac{\partial V(\tilde{x}_b(t_0))}{\partial x} f(\tilde{x}_b(t_0), u^*(x_0+\delta), 0) \right| \\ &\leq -\alpha_3(|\tilde{x}_b(t_0)|) + L'_x|x_b(\tau) - x_b(t_0) - \delta| + L'_w\theta \\ &\leq -\alpha_3(\alpha_2^{-1}(\rho'_e)) + L'_x M\Delta + L'_x|\delta| + L'_w\theta \end{aligned} \tag{41}$$

since $\tilde{x}_b(t_0) \in \Omega_\rho/\Omega_{\rho'_e}$, where the first inequality follows from adding and subtracting $\frac{\partial V(\tilde{x}_b(t_0))}{\partial x} f(\tilde{x}_b(t_0), u^*(x_0 + \delta), 0)$ from the right-hand and using Eq. 40. If Eq. 35 holds, then $\dot{V}(x_b(\tau)) \leq -\epsilon'_w/\Delta$ for $\tau \in [0, t_1)$, so that $V(x_b(t)) \leq V(x_0)$, $\forall\ t \in [0, t_1)$, and therefore $x_b(t) \in \Omega_{\rho_{samp2}}$.

Case 3. If $x_0 \in \Omega_{\rho_{samp}}/\Omega_{\rho'_e}$, then from Eq. 37, $V(x_b(t)) \leq \rho_{samp2}$, $\forall\ t \in [0, t_1)$.

Case 4. When $x_0 + \delta \in \Omega_\rho/\Omega_{\rho'_e}$ but $x_0 \in \Omega_{\rho'_e}$, Eq. 13i is applied. From the proof for Case 2, this causes $V(x_b(t)) \leq V(x_0)$, $\forall\ t \in [0, t_1)$ if Eq. 35 holds and $x_0 \in \Omega_{\rho'_e}/\Omega_{\rho_s}$, such that $V(x_b(t)) \leq \rho' < \rho_{samp2}$, $\forall\ t \in [0, t_1)$. If $x_0 \in \Omega_{\rho_s}$, then $x_b(t) \in \Omega_{\rho_{\min}} \subset \Omega_{\rho_{samp2}}$, for $t \in [t_0, t_1)$, from Eq. 36.

The above indicates feasibility of the LEMPC at t_0 and closed-loop stability from $[0, t_1)$ in the sense that the closed-loop state is maintained within $\Omega_{\rho_{samp2}}$ within that timeframe if $x(t_0) \in \Omega_{\rho_{samp2}}$. To demonstrate the result of the theorem (i.e., that $x(t) \in \Omega_{\rho_{samp2}}$ for all $t \geq 0$ when the conditions of the theorem are met), we examine the case at t_1. At t_1, one of Cases 1-4 holds again, and so the state at t_2 will again be within $\Omega_{\rho_{samp2}}$. Applying the above recursively establishes that $x(t) \in \Omega_{\rho_{samp2}}$ for all times, and the state measurement at every sampling time is in Ω_ρ from Eq. 38.

C. Stability and Feasibility Analysis: Differences Between Measurement Noise and False Sensor Measurements

In this section, we elucidate the implications of the stability results presented above for the case of cyberattacks on the state measurements. In particular, we now consider the case that x_a and x_b (with slight abuse of notation) are state trajectories resulting from two different inputs $u^*(x_0)$ and $u^*(x_0 + \delta)$ being applied to the system of Eq. 1 from $x_a(t_0) = x_b(t_0) = x_0$, where now $|\delta|$ may be larger than ϕ (i.e., it reflects offset of the measured state from the actual state x_0 due to a falsified sensor measurement, which is not related to the sensor noise assumptions of Section II-B). In this case, Propositions 1-3 continue to hold for the new definitions of x_a and x_b, as they were derived considering an arbitrary $|\delta|$ as long as $x_0 + \delta \in \Omega_\rho$ (part of a cyberattack detection mechanism could include flagging a state measurement as a false measurement if the state measurement is not in Ω_ρ). The question to be addressed is whether the conditions of Theorem 1 are sufficient to ensure that the closed-loop state is maintained within $\Omega_{\rho_{samp2}}$ for all times if $x(t_0) \in \Omega_{\rho_{samp2}}$, as held for the measurement noise case in Theorem 1. The goal of this discussion is to utilize a theoretical construct that allows stability guarantees to be made in the presence of measurement noise, but would not allow the same guarantees to be made in the presence of false sensor measurements, to elucidate some of the differences between false sensor measurements and measurement noise. In particular, it reveals that false sensor measurement cyberattacks are not equivalent to measurement noise, or capable of being always treated in the same fashion.

The recursive feasibility and stability properties in Theorem 1 arise from knowledge that at the beginning of every sampling period, the state measurement is within $|\delta|$ of its true value (Eq. 2). In particular, the proof of Theorem 1 requires that Eqs. 34, 35, and 38 hold; these require that $|\delta|$ be sufficiently small. For the measurement noise case, the maximum value that $|\delta|$ can take is ϕ, which could be adjusted practically to ensure that it is sufficiently small by varying, for example, the sensing equipment. Cyberattacks would not necessarily maintain the state measurement within a small range of x_0; therefore, it can be expected that in general, Theorem 1 does not provide a framework for guaranteeing closed-loop stability in the presence of false sensor measurement cyberattacks.

If it could be guaranteed that at t_0, the only cyberattacks which could occur were those for which the difference δ between the state measurement and actual state meets the conditions of Theorem 1, then for the subsequent sampling period, the closed-loop state would be maintained in $\Omega_{\rho_{samp2}}$. The conditions of Theorem 1 suggest that a conservative design of the controller of Eq. 13 may be selected that would guarantee closed-loop stability for a sampling period after an attack for a number of different values of δ (i.e., for different magnitudes of the false state measurement differing from the actual measurement). To attempt to reduce the conservatism in this approach, one could consider making state predictions at every sampling time by simulating the nominal model of Eq. 1 for a sampling period from the last sensor measurement. Then, the difference between the state measurement and the prediction could be checked. If an auxiliary detection mechanism exists that always identifies a cyberattack on the sensor measurements in one sampling period, then we can be sure that if no cyberattack was detected before t_k, the state measurement at t_{k-1} was subject only to bounded measurement noise (i.e., $|\tilde{x}_b(t_{k-1}) - x_b(t_{k-1})| \leq \phi$). We will use this in developing an estimate of $x_b(t_k)$ via the nominal model so that we flag sensor measurements for which $|\tilde{x}_b(t_k) - x_b(t_k)| > |\delta|$ as false. This will ensure that at t_k, if an attack has occurred, it can be flagged as an attack and a backup policy can be implemented; otherwise, $|\tilde{x}_b(t_k) - x_b(t_k)| \leq |\delta|$ so that for the subsequent sampling period, if the conditions of Theorem 1 hold for that δ, the closed-loop state is maintained in $\Omega_{\rho_{samp2}}$. Because of the auxiliary detection mechanism, it is assumed that an attack will be found by t_{k+1}, permitting mitigating actions.

We make this precise (considering measurements $\tilde{x}_b(t_{k-1})$ and $\tilde{x}_b(t_k)$, and $\hat{x}_b(t)$ to denote the predicted state from the nominal model of Eq. 1 initialized from $\tilde{x}_b(t_{k-1})$): given that $|\tilde{x}_b(t_{k-1}) - x_b(t_{k-1})| \leq \phi$, Proposition 2 gives:

$$|x_b(t_k) - \hat{x}_b(t_k)| \leq f_W(\phi, \Delta) \tag{42}$$

Using this, we have that:

$$\begin{aligned} |x_b(t_k) - \tilde{x}_b(t_k)| &\leq |x_b(t_k) - \hat{x}_b(t_k) + \hat{x}_b(t_k) - \tilde{x}_b(t_k)| \\ &\leq f_W(\phi, \Delta) + |\hat{x}_b(t_k) - \tilde{x}_b(t_k)| \end{aligned} \tag{43}$$

If we flag every case where $|\hat{x}_b(t_k) - \tilde{x}_b(t_k)| > \nu_1$, for $\nu_1 > 0$, as a cyberattack, then:

$$|x_b(t_k) - \tilde{x}_b(t_k)| \leq f_W(\phi, \Delta) + \nu_1 \tag{44}$$

if no attack is flagged. Finally, if ν_1, ϕ, and Δ are chosen such that $f_W(\phi, \Delta) + \nu_1 \leq |\delta|$ for some δ for which the conditions of Theorem 1 hold, this ensures that $|x_b(t_k) - \tilde{x}_b(t_k)| \leq |\delta|$ so that closed-loop stability is maintained over the next sampling period even if there is a cyberattack on the sensor measurements for which $|x_b(t_k) - \tilde{x}_b(t_k)| \leq |\delta|$.

Closed-loop stability for all times after attacks begin to occur (i.e., if no auxiliary detection method is used) may not be able to be guaranteed via the above method even if the condition $|\hat{x}(t_k) - \tilde{x}_b(t_k)| \leq \nu_1$ continues to hold at subsequent sampling periods. This is because the above method relies on predictions of the state of Eq. 1 from the prior sampling time. A fundamental difference between a cyberattack and measurement noise is that the "approximate" value of the state is never obtained in an attack. An attacker could ensure, for example, that at every sampling time, the difference between $\tilde{x}_b(t_k)$ and $\hat{x}_b(t_k)$ is less than $|\delta|$; however, if the state measurement used at the last sampling time was also falsified, there is no guarantee that this method of making predictions is keeping $|x_b(t_k) - \tilde{x}_b(t_k)| < |\delta|$ at each sampling time. Part of the motivation for utilizing the input rate of change constraints in Eq. 13 is that they help to prevent $u^*(x_0)$ and $u^*(x_0 + \delta)$ from differing from one another too significantly over a sampling period, which may be helpful for allowing $|\delta|$ to be larger in an attack while still satisfying, for example, Eq. 34.

Remark 1: The analysis above helps to show why some alternative strategies incorporating randomization in the traditional LEMPC formulation of Eq. 12 as a means for dealing with the cyberattack may be less attractive than Eq. 13. For example, consider a set of state measurements available to a controller at a given time t_0. A potential method that could be utilized to attempt to thwart a cyberattack in which false sensor measurements could be provided to any sensor could be to have the controller randomly select which sensors would provide state measurements to Eq. 12 from a set of physical sensors, with the remainder of the states for which no measurements are obtained coming from estimates. The implementation of such a network and methodology could make it difficult for the cyberattacker to know if the supplied false values will affect the process, since it is presumed that the attacker would not be aware of which sensors would be providing the state measurement at time t_k. However, if the cyberattacker does manage to select sensors from which the state measurements are being given as the initial condition in Eq. 12c, the resulting deviations of the state trajectory from the trajectory it otherwise would have taken could cause the process state to exit the stability region.

IV. Chemical Process Example

In this section, we demonstrate concepts discussed above for a process under an EMPC design without Lyapunov-based stability constraints (the continuous stirred tank reactor (CSTR) in [6]). Reactant is introduced into the reactor through an inlet stream with flow rate F, temperature T_0, and initial concentration C_{A0}. A heating jacket provides heat at rate Q. The following ordinary differential equations, describe the concentration of reactant A (C_A) and temperature T within the reactor over time:

$$\begin{aligned}\frac{dC_A}{dt} &= \frac{F}{V_R}(C_{A0} - C_A) - k_0 e^{-E/RT} C_A^2 \\ \frac{dT}{dt} &= \frac{F}{V_R}(T_0 - T) - \frac{\Delta H k_0}{\rho_R C_p} e^{-E/RT} C_A^2 + \frac{Q}{\rho_R C_p V_R}\end{aligned} \tag{45}$$

where k_0, V_R, ρ_R, E, R, and C_p are, respectively, the pre-exponential constant, volume of fluid in the reactor, fluid density, reaction activation energy, gas constant, and heat capacity. The inputs are the inlet reactant concentration $C_{A0} \in [0.5, 7.5]$ kmol/m^3 and heat rate supplied $Q \in [-50.0, 50.0]$ MJ/h. The process parameters are presented in [6]. To control the process, an EMPC is utilized with the stage cost $L_e = -k_0 e^{\frac{-E}{RT(t)}}(C_A(t))^2$. The simulations were initialized from $C_A(t_0) = 2.0$ kmol/m^3 and $T(t_0) = 425.0$ K and run at one sampling time with a sampling period of length 0.01 h, with a prediction horizon of $N = 10$ and an integration step of 10^{-3} h used to simulate the process with the Explicit Euler numerical integration method. The simulations were performed in MATLAB using fmincon. To examine the effect of a cyberattack over a sampling period, false sensor readings of the concentration, $C_{A,False}$, and temperature, T_{False}, were provided to the EMPC. Values of $(C_{A,False}, T_{False})$ as follows were tested: (1.8,425), (2,420), (2,425), (2,430), (3,425), and (4,425), with concentration in kmol/m^3 and temperature in K. The inputs computed, and therefore also the state trajectories over the subsequent sampling period, were about the same as when the true state measurement was provided. To exemplify the discussion regarding state prediction error over time without feedback, we also present the results (Fig. 1) for the case that the EMPC is simulated for 0.1 h with the false state measurement at each sampling time being 0.2 kmol/m^3 and 5 K above the predicted value (predicted from the false measurement).

Acknowledgment

Financial support from the Wayne State College of Engineering start-up funding, Wayne State Research Opportunities for Engineering Undergraduates, and NSF CNS-1932026 is gratefully acknowledged.

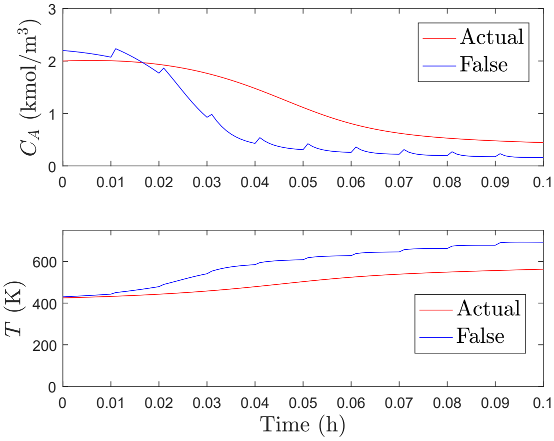

Fig. 1. Trajectories of C_A and T for 0.1 h under a cyberattack scenario with a false measurement offset from a predicted value. “Actual” signifies the actual state, and “False” signifies the predictions starting from a false measurement at each t_k.

References

[1] R. Langner, “Stuxnet: Dissecting a cyberwarfare weapon,” *IEEE Security & Privacy*, vol. 9, pp. 49–51, 2011.

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

[3] H. Fawzi, P. Tabuada, and S. Diggavi, “Secure estimation and control for cyber-physical systems under adversarial attacks,” *IEEE Transactions on Automatic Control*, vol. 59, pp. 1454–1467, 2014.

[4] Z. Wu, F. Albalawi, J. Zhang, Z. Zhang, H. Durand, and P. D. Christofides, “Detecting and handling cyber-attacks in model predictive control of chemical processes,” *Mathematics*, vol. 6, p. 22 pages, 2018.

[5] I. Kiss, B. Genge, and P. Haller, “A clustering-based approach to detect cyber attacks in process control systems,” in *Proceedings of the IEEE 13th International Conference on Industrial Informatics*, Cambridge, UK, 2015, pp. 142–148.

[6] M. Ellis, H. Durand, and P. D. Christofides, “A tutorial review of economic model predictive control methods,” *Journal of Process Control*, vol. 24, pp. 1156–1178, 2014.

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

[8] M. A. Müller, L. Grüne, and F. Allgöwer, “On the role of dissipativity in economic model predictive control,” *IFAC-PapersOnLine*, vol. 48, pp. 110–116, 2015.

[9] M. Heidarinejad, J. Liu, and P. D. Christofides, “Economic model predictive control of nonlinear process systems using Lyapunov techniques,” *AIChE Journal*, vol. 58, pp. 855–870, 2012.

[10] H. Durand, “A nonlinear systems framework for cyberattack prevention for chemical process control systems,” *Mathematics*, vol. 6, p. 44 pages, 2018.

[11] H. Durand, M. Ellis, and P. D. Christofides, “Economic model predictive control designs for input rate-of-change constraint handling and guaranteed economic performance,” *Computers & Chemical Engineering*, vol. 92, pp. 18–36, 2016.

[12] H. K. Khalil, *Nonlinear Systems*, 3rd ed. Upper Saddle River, NJ: Prentice Hall, 2002.

[13] J. L. P. Mhaskar and P. D. Christofides, *Fault-Tolerant Process Control: Methods and Applications*. London, England: Springer-Verlag, 2013.

[14] M. Ellis, J. Zhang, J. Liu, and P. D. Christofides, “Robust moving horizon estimation based output feedback economic model predictive control,” *Systems & Control Letters*, vol. 68, pp. 101–109, 2014.