Wayne State University

Chemical Engineering and Materials Science Faculty Research Publications

Chemical Engineering and Materials Science

9-5-2024

Profit Considerations For Nonlinear Control-Integrated Cyberattack Detection On Process Actuators

Keshav Kasturi Rangan
Wayne State University, keshav@wayne.edu

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

Follow this and additional works at: https://digitalcommons.wayne.edu/cems_eng_frp

Part of the Controls and Control Theory Commons, Information Security Commons, and the Process Control and Systems Commons

Recommended Citation

Rangan, K.K.; Durand, H. Profit Considerations For Nonlinear Control-Integrated Cyberattack Detection On Process Actuators. IFAC Papers OnLine 58(14), 2024, 592-597. https://doi.org/10.1016/j.ifacol.2024.08.401

This Article is brought to you for free and open access by the Chemical Engineering and Materials Science at DigitalCommons@WayneState. It has been accepted for inclusion in Chemical Engineering and Materials Science Faculty Research Publications by an authorized administrator of DigitalCommons@WayneState.

Available online at www.sciencedirect.com

ScienceDirect

IFAC PapersOnLine 58-14 (2024) 592–597

Profit Considerations For Nonlinear Control-Integrated Cyberattack Detection On Process Actuators[★]

Keshav Kasturi Rangan [*] **Helen Durand** [**]

[*] *Wayne State University, 42 W. Warren Ave. Detroit, MI 48202, USA (e-mail: keshav@wayne.edu).*
[**] *Wayne State University, 42 W. Warren Ave. Detroit, MI 48202, USA(e-mail: helen.durand@wayne.edu)*

Abstract: Prior research from our group developed a control-integrated active actuator cyberattack detection strategy. This strategy continuously probed for cyberattacks by updating target steady-states at every sampling time and then moving the process state toward these over the subsequent sampling period. Attacks were flagged if a Lyapunov function around the target steady-state did not decrease over a sampling period. This strategy had the benefit of ensuring safety of the process until an attack was detected. However, the continuous probing for attacks could decrease profit from the process compared to not probing for the attacks, which could limit the attractiveness of the method in practice. This work marks our first step toward attempting to develop a framework for modifying this detection strategy to make guarantees that the profit over a sampling period would be no worse than that of a stabilizing controller. This is achieved through utilizing two auxiliary controllers, in addition to the one which facilitates the attack-probing, with constraints on profits in the various controllers to enable the profit proofs over a sampling period (in the absence of disturbances) to be developed. A process reactor example is used to demonstrate the implementation of the detection strategy.

Copyright © 2024 The Authors. This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0/)

Keywords: Advanced process control, Nonlinear predictive control, Cyberattack detection, Lyapunov methods, Profitability of stabilized nonlinear systems

1. INTRODUCTION

An Industry 4.0 setup is designed to increase automation and improve operational efficiency. However, it can also lead to more opportunities for cyberattackers to attack a process. This has led to investigations focused on practical issues (e.g., classifications and potential attack surfaces for cyberattacks on networked control systems (Sánchez et al., 2019)), as well as more theory-focused techniques for cyberattack-handling (e.g., detection and cyberattack-handling techniques in the context of distributed model predictive control (MPC) for linear systems (Velarde et al., 2017)). On the theoretical side, one of the major directions for cyberattack detection has been active attack detection, which refers to the injection of specific input policies that perturb the optimal operation of a system to flag cyberattacks (Satchidanandan and Kumar, 2016). These can be implemented by either continuously perturbing the system or switching to perturbing actions at certain times (Narasimhan et al., 2022). Attacks can be considered on various control components, including sensors and actuators. Our prior work has considered detection and handling strategies for both sensor attacks (e.g., (Rangan et al., 2021; Oyama et al., 2023)) and actuator attacks (Rangan et al., 2022). Our prior strategies have focused on utilizing an advanced control strategy called Lyapunov-based economic model predictive control (LEMPC) to detect these types of attacks due to its closed-loop stability properties even in the presence of sufficiently small measurement noise (and thus also sensor attacks) and disturbances (and thus also actuator attacks). As an example, the strategy for handling actuator attacks in (Rangan et al., 2022) involves developing a series of steady-states over time and then driving the closed-loop state toward each for a sampling period. This ensures that the Lyapunov function around each steady-state should decrease over a sampling period, enabling an attack on actuators to be detected if it does not, and also ensuring that any undetected actuator attacks had to cause the Lyapunov function to decrease and thus could not have driven the closed-loop state out of a safe operating region.

Despite the safety benefits of the strategy in (Rangan et al., 2022) when actuators are attacked, the constant probing required for achieving these safety benefits in the presence of attacks may prevent the process from operating in an economically-optimal fashion. As a result, (Rangan et al., 2022) suggested that a potential idea for overcoming this issue was to utilize an auxiliary economic model predictive control (Ellis et al., 2014; Rawlings et al., 2012) scheme to determine the steady-states that should be designed at each sampling time, with the hope that guiding the closed-loop state toward such steady-states might en-

[★] Financial support from the Air Force Office of Scientific Research award number FA9550-19-1-0059, National Science Foundation CBET-1839675, CNS-1932026, and CBET-2143469, and Wayne State University is gratefully acknowledged.

2405-8963 Copyright © 2024 The Authors. This is an open access article under the CC BY-NC-ND license.
Peer review under responsibility of International Federation of Automatic Control.
10.1016/j.ifacol.2024.08.401

hance economic operation compared to other ideas for generating the steady-states (e.g., selecting them randomly). Though this strategy sounds promising, no work was performed in (Rangan et al., 2022) to attempt to theoretically evaluate the ability of such a methodology to keep profits above the value they would take with alternative control laws. The development of theories which indicate how to prevent profit reduction during active attack detection is critical to characterizing such methods and articulating their potential use cases. This work marks our first step toward addressing the question of ensuring profits for an active attack strategy like that in (Rangan et al., 2022).

2. PRELIMINARIES

2.1 Notation

x^T and $|x|$ signify the transpose and Euclidean norm of a vector x. A class $\mathcal{K}$ function $\alpha : [0, a) \rightarrow [0, \infty)$, where $\alpha(0) = 0$, is strictly increasing. $x \in A/B$ signifies the set $\{x \in \mathbb{R}^n : x \in A, x \notin B\}$. A level set of a positive definite function V is denoted by $\Omega_\rho := \{x \in \mathbb{R}^n : V(x) \leq \rho\}$. $\mathbb{R}_+$ signifies the set of non-negative real numbers.

2.2 Class of Systems

We consider the following class of nonlinear systems:

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

where $x \in X \subset \mathbb{R}^n$ and $u \in U \subset \mathbb{R}^m$ represent the state and input vectors. f is assumed to be a locally Lipschitz nonlinear vector function of its arguments ($X \times U$). The system of Eq. 1 is assumed to be stabilizable such that there exists a controller $h(x) \subset \mathbb{R}^m$, a sufficiently smooth Lyapunov function $V : \mathbb{R}^n \rightarrow \mathbb{R}_+$, and class $\mathcal{K}$ functions, $\alpha_j(\cdot)$, $j = 1, \ldots, 4$, such that:

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

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

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

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

$\forall x \in D \subset \mathbb{R}^n$. $\Omega_\rho \in D$ represents the "stability region" under the controller $h(x)$. D is an open neighborhood of the origin. Using the assumptions of a smooth Lyapunov function V, and a locally Lipschitz function f, the following equations are obtained:

$$|f(x, u) - f(x', u')| \leq L_x|x - x'| + L_u|u - u'| \tag{3a}$$

$$\left|\frac{\partial V(x)}{\partial x} f(x, u) - \frac{\partial V(x')}{\partial x'} f(x', u)\right| \leq L'_x|x - x'| \tag{3b}$$

$$|f(x, u)| \leq M_f \tag{4}$$

$\forall x, x' \in \Omega_\rho \subset X$, and $u, u' \in U$, where L_x, L'_x, L_u, and M_f are positive constants.

2.3 Lyapunov-Based Economic Model Predictive Control (LEMPC)

This work utilizes an optimization-based control design known as LEMPC (Heidarinejad et al., 2012) written as:

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

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

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

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

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

$$V(\tilde{x}(t)) \leq \rho_e, \ \ \forall\, t \in [t_k, t_{k+N}), \quad \text{if } \tilde{x}(t_k) \ \in \ \Omega_{\rho_e} \tag{5f}$$

$$\frac{\partial V(\tilde{x}(t_k))}{\partial \tilde{x}} f(\tilde{x}(t_k), u(t_k)) \leq \frac{\partial V(\tilde{x}(t_k))}{\partial \tilde{x}} f(\tilde{x}(t_k), h(\tilde{x}(t_k))), \quad \text{if } \ \tilde{x}(t_k) \in \Omega_\rho/\Omega_{\rho_e} \tag{5g}$$

where $u(t) \in S(\Delta)$ is a piecewise constant input applied over a sampling period, Δ. Eq. 5a is the objective to be minimized over a prediction horizon of length $N\Delta$. Eq. 5b represents the process model. At every sampling time, state prediction $\tilde{x}(t)$ is reset to the measurement (Eq. 5c). Eqs. 5d-5e are state and input constraints. Eq. 5f allows the economic operation of the process within Ω_{ρ_e}. If $\tilde{x}(t_k) \in \Omega_\rho/\Omega_{\rho_e}$ is satisfied, then Eq. 5f is switched to Eq. 5g. Eq. 5g represents the contractive Lyapunov constraint that reduces V at least as much as when $h(x)$ is applied. An optimization formulation that has all the constraints in Eq. 5 except for Eq. 5f represents a Lyapunov-based model predictive controller (LMPC) that drives the state to the steady-state (Mhaskar et al., 2006).

3. ACTIVE CYBERATTACK DETECTION USING LEMPC WITH PROFIT CONSIDERATIONS

As mentioned in Section 1, active detection strategies are designed to detect cyberattacks by perturbing the steady-state optimal operation of a process, potentially reducing profits. However, it can be challenging to theoretically compare the profits of a process that does not use a cyberattack-probing detection strategy with those of one that uses it to analyze the extent to which the probing detection strategy reduces profits.

This may make active detection methods undesirable for enhancing plant security. In this work, we seek to develop a strategy for analyzing the impact of active attack detection on process profitability by modifying the active detection strategy discussed in (Rangan et al., 2022). The strategy to be presented will ensure that over any sampling period, the economic performance of an active detection strategy that can guarantee safety at all times in the absence of attacks is no worse than that of an LMPC over the same time period. These proofs are made in the absence of disturbances to focus on characterizing the effects of active cyberattack detection methods on chemical processes and building toward detection strategies that explicitly account for profitability while carrying out their detection goals. A consequence of the proposed formulation is that, compared to (Rangan et al., 2022), the proposed profit-focused methods may not be able to detect all actuator attacks that could increase the Lyapunov function values. However, analyzing the safety implications of an undetected attack in such a scenario can be a focus of future work. Profit proofs are of greatest interest in the absence of attacks, as the key issue which motivates their investigation is the disruption of active attack detection to normal operation.

The active actuator attack detection strategy in (Rangan et al., 2022) detects actuator attacks by creating a series of steady-states (i^{th} steady-states, $i = 1, 2, \ldots$, one for each sampling period of operation) that the process should track. This series of steady-states is selected such that a Lyapunov function designed around each steady-state should decrease between one sampling period and the next. If it does not, an attack is flagged. To move the state toward these steady-states, a new LMPC formulation is used at every sampling period in Rangan et al. (2022). It is desirable to carefully choose this series of steady-states to avoid a significant reduction in profits due to an active cyberattack detection policy. One method suggested in Rangan et al. (2022) for selecting these "pseudo" steady-states with profit considerations in mind is to determine them using an auxiliary LEMPC (an A-LEMPC). Since the LEMPC optimizes profits, the state that it predicts at the end of each sampling period can be considered to be an economically-optimal "pseudo" steady-state to reach over a sampling period. Thus, the state at the end of one sampling period in the A-LEMPC is used as the next steady-state which should be tracked in the cyberattack-probing strategy. The LMPC designed to move the closed-loop state of the process toward the i^{th} "pseudo" steady-state is referred to as the i^{th} LMPC. Thus, the implementation strategy suggested in Rangan et al. (2022) for attempting to limit losses during active detection was to probe for cyberattacks by designing a series of steady-states and new i^{th} LMPC formulations to track these states at each sampling period. In Rangan et al. (2022), this strategy was presented without an attempt to theoretically analyze the impact on profits during the active attack detection compared to not probing for attacks.

In this work, we seek to develop theoretical guarantees on the profit obtained over a single sampling period while performing active attack detection. Though we are motivated by the active attack detection methodology in Rangan et al. (2022), that methodology is not formulated in a manner that enables explicit guarantees on profits to be made, because no constraints on profits tie the i^{th} LMPC formulations to those of the A-LEMPC. Thus, we formulate a new methodology inspired by the active attack detection strategy in Rangan et al. (2022) but evaluated in the absence of disturbances to determine the effects (on profitability) of probing for attacks by using an optimization-based controller that tracks a series of steady-states. However, we pair it with both: 1. an auxiliary LMPC (A-LMPC) against which we wish to compare the profits over a sampling period (i.e., we wish to demonstrate that the cyberattack-probing strategy can, over one sampling period, produce an economic performance at least as good as that of the auxiliary LMPC), and 2. an auxiliary LEMPC (A-LEMPC) that is used to produce steady-states for the series of i^{th} LMPC's to track, consequently enabling them to have the potential to outperform the auxiliary LMPC. The concept of using a cascade of controllers in economic performance analysis for model predictive control, with constraints in the A-LEMPC and i^{th} LMPC's designed to attempt to promote profitability of operation under the active cyberattack probing strategy, is inspired by strategies in (Heidarinejad et al., 2013), which were developed without considering active attack probing. Our profitability analysis in this work provides a step toward elucidating the conditions under which active detection policies may not create severe profit loss.

3.1 Formulation of Detection Strategy

As mentioned above, our proposed strategy for ensuring profitability during cyberattack probing over any sampling period uses three optimization-based controllers: an A-LMPC that is solved first at every sampling period to determine a minimum profit that should be achieved during cyberattack probing over the following sampling period, an A-LEMPC that finds a steady-state for the i^{th} LMPC to track over each sampling period, and the i^{th} LMPC, which computes stabilizing control actions for the process that drive it toward the "pseudo" steady-state computed by the A-LEMPC, which is similar in concept to the active attack detection policy in Rangan et al. (2022). Because the A-LMPC is meant be the profit benchmark as a control strategy that is unaffected by the cyberattack probing method, it is formulated according to the standard LMPC formulation (Eq. 5 without Eq. 5f, and with Eq. 5g applied at every sampling time).

The predictions of the closed-loop state under the A-LMPC (denoted by the state trajectory $\tilde{x}_{al}(t)$, $t \in [t_k, t_{k+N})$) and the input policy computed by the A-LMPC over the prediction horizon (denoted by $u_{al}(t)$, $t \in [t_k, t_{k+N})$) are sent to the A-LEMPC. These are then used by the A-LEMPC to predict the profit that the A-LMPC was able to achieve under its optimal control input trajectory. This is then used in forming a constraint in the A-LEMPC that requires that the profit of the A-LEMPC be at least as high as that of the A-LMPC over a sampling period (corresponding to the relevant time period for computing a steady-state to send to the i^{th} LMPC), as follows:

$$\max_{u_{ae}(t)\in S(\Delta)} \int_{t_k}^{t_{k+N}} L_e(\tilde{x}_{ae}(\tau), u_{ae}(\tau))\, d\tau \tag{6a}$$

$$\text{s.t. } \dot{\tilde{x}}_{ae}(t) = f(\tilde{x}_{ae}(t), u_{ae}(t)) \tag{6b}$$

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

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

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

$$V_A(\tilde{x}_{ae}(t)) \le \rho_{e_A},\ \ \forall\, t \in [t_k, t_{k+N}),\quad \text{if } \tilde{x}_{ae}(t_k)\ \in\ \Omega_{\rho_{e_A}} \tag{6f}$$

$$\frac{\partial V_A(\tilde{x}_{ae}(t_k))}{\partial x_{ae}} f(\tilde{x}_{ae}(t_k), u_{ae}(t_k)) \le \frac{\partial V_A(\tilde{x}_{ae}(t_k))}{\partial x_{ae}}\ f(\tilde{x}_{ae}(t_k), h_A(\tilde{x}_{ae}(t_k))),\quad \text{if } \ \tilde{x}_{ae}(t_k) \in \Omega_{\rho_A}/\Omega_{\rho_{e_A}} \tag{6g}$$

$$\int_{t_k}^{t_{k+1}} L_e(\tilde{x}_{ae}(\tau), u_{ae}(\tau))\, d\tau \ge \int_{t_k}^{t_{k+1}} L_e(\tilde{x}_{al}(\tau), u_{al}(\tau))\, d\tau \tag{6h}$$

where the notation in Eqs. 6a-6g follows that in Eq. 5, except that the state predictions under the input trajectory u_{ae} computed by the A-LEMPC are denoted by $\tilde{x}_{ae}$, and the stability region and its subset are written as ρ_A and ρ_{e_A} to distinguish them from the values used in the i^{th} LMPC. Eq. 6h provides the bound on the profits noted above.

Eq. 6 provides process states, $\tilde{x}_{ae}(t_{k+1})$ at every sampling time t_k to be used as "pseudo" steady-states by the i^{th} LMPC. This is called the i^th LMPC formulation since a new formulation is determined at every sampling time, $i = 1, 2, \ldots$. Each i^{th} LMPC formulation is designed around a new i^{th} "pseudo" steady-state. To connect the profitability of this strategy with that of the A-LEMPC, an explicit requirement is made that the profits over a sampling period be lower bounded by those of the A-LMPC and upper bounded by those of the A-LEMPC. This creates the following i^{th} LMPC formulation:

$$\max_{u_i(t) \in S(\Delta)} \int_{t_k}^{t_{k+1}} L_e(\tilde{x}_i(\tau), u_i(\tau))\, d\tau \tag{7a}$$

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

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

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

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

$$\begin{aligned} &\frac{\partial V_i(\tilde{x}_i(t_k))}{\partial x} f_i(\tilde{x}_i(t_k), u_i(t_k)) \\ &\qquad \leq \frac{\partial V_i(\tilde{x}_i(t_k))}{\partial x} f_i(\tilde{x}_i(t_k), h_i(\tilde{x}_i(t_k))) \end{aligned} \tag{7f}$$

$$\begin{aligned} &\int_{t_k}^{t_{k+1}} L_e(\tilde{x}_{al}(\tau), u_{al}(\tau))\, d\tau \\ &\qquad \leq \int_{t_k}^{t_{k+1}} L_e(\tilde{x}_i(\tau), u_i(\tau))\, d\tau \end{aligned} \tag{7g}$$

$$\begin{aligned} &\int_{t_k}^{t_{k+1}} L_e(\tilde{x}_i(\tau), u_i(\tau))\, d\tau \\ &\qquad \leq \int_{t_k}^{t_{k+1}} L_e(\tilde{x}_{ae}(\tau), u_{ae}(\tau))\, d\tau \end{aligned} \tag{7h}$$

where $\tilde{x}_i(t_k)$ and f_i are both written in deviation variable form with respect to the i^{th} steady-state ($i = 1, 2, \ldots$) which is updated at every sampling time. $x_i(t_k)$ and $\tilde{x}_i(t_k)$ represent the measured and predicted states in deviation from the i^{th} steady-state. Similarly, u_i, X_i, and U_i are all expressed in deviation variable form with respect to the corresponding i^{th} steady-state. The control action computed by the i^{th} LMPC is the control action that is actually applied to the process. Eqs. 7g and 7h represent the profit constraints. In the case that the i^{th} LMPC is infeasible, the A-LMPC control action is applied to the process instead. The potential that the i^{th} LMPC maybe infeasible could mean that the Lyapunov function may not be guaranteed to decrease under sufficient conditions like those in Rangan et al. (2022). When it is infeasible, we will still consider monitoring the Lyapunov function decease and using it as a flag for cyberattack detection since the method in Rangan et al. (2022) inspires this work. However, we also note that when the i^{th} LMPC is not feasible, an increase in the Lyapunov function value could create false cyberattack detection alarms in certain scenarios.

3.2 Implementation of Detection Strategy

The implementation strategy is as follows:

(1) The A-LMPC (Eq. 5) receives a state measurement $(x(t_k))$ to evaluate the input and stage cost of the process over Δ and N. Go to Step 2.
(2) The A-LEMPC (Eq. 6) receives $x(t_k)$ along with the associated economic costs for the A-LMPC applied over Δ and N. Go to Step 3.
(3) If $x(t_k) \in \Omega_{\rho_e}$, go to Step 3(i). Else, go to Step 3(ii). (i) The A-LEMPC maximizes the economic cost function within the region Ω_{ρ_e}. Go to Step 4. (ii) The A-LEMPC activates the contractive constraint of Eq. 6g at t_k. Go to Step 4.
(4) The state predicted by the A-LEMPC along with the economics of both auxiliary formulations are sent to the i^{th} LMPC. Go to Step 5.
(5) Conditions to be satisfied by $\tilde{x}_{ae}(t_{k+1})$ before being accepted as the i^{th} steady-state: (i) A region Ω_{ρ_i} must be determined around the i^{th} steady-state such that $\Omega_{\rho_i} \subset \Omega_\rho$. (ii) $x_i(t_k), \tilde{x}_{ae}(t_{k+1}) \in \Omega_{\rho_i}$, to ensure that the actual process state does not leave the safe region of operation. (iii) The steady-state input corresponding to $\tilde{x}_{ea}(t_{k+1})$ must be within U_i (iv) $x_i(t_k) \notin \Omega_{\rho_{s,i}}$, for the Lyapunov function to decrease, if the i^{th} LMPC is feasible. (v) If the i^{th} LMPC is feasible, replace its input with that of the A-LMPC. Go to Step 6.
(6) A cyberattack is flagged if V_i did not decrease over the sampling period. Go to Step 7.
(7) $(t_k \leftarrow t_{k+1})$. Go to Step 1.

3.3 Proofs for the Detection Strategy

This section makes theoretical guarantees related to 1) recursive feasibility of the A-LMPC and A-LEMPC, 2) stability of the system of Eq. 1 operated under the implementation strategy of Section 3.2 in the absence of attacks, and 3) profitability of operation under the implementation strategy of Section 3.2. Due to the potential infeasibility of the i^{th} LMPC, this strategy cannot guarantee that cyberattacks are detected and that no false alarms are raised, but this represents a step toward integrating an active attack-probing strategy with economics, even if some of the guarantees that the method can detect attacks using the decrease in the Lyapunov function are lost in the attempt to integrate with profits. Indeed, in the no-noise case considered, cyberattack detection would become trivial as any slight deviation of the state measurement from a perfect prediction of the state would already indicate the presence of an attack. Furthermore, since actuator attacks are considered and the profit proofs rely on the control actions being those computed by the controllers designed in this manuscript with the various profit-based constraints, the proofs of profits would not hold in the presence of attacks on the actuators.

In the following proof, functions such as α_j, $j = 1, 2, 3, 4$, and h, or constants like M_f, L_x, L'_x, and L_u will have an additional subscript 'A' or 'i' to indicate if the terms are associated with an auxiliary controller formulation or the i^{th} LMPC formulation.

Theorem 1. Consider the closed-loop system of Eq. 1 under the implementation strategy of Section 3.2. The control actions $h_A(\cdot)$ and $h_i(\cdot)$ are assumed to satisfy the inequalities in Eqs. 2a-2d. If there exist $\epsilon'_{W_i} > 0$,

$\Delta > 0$, $\Omega_{\rho_i} \subset \Omega_{\rho_A} \subset X$, $\Omega_{\rho_{s_A}} \subset \Omega_{\rho_{\min,A}} \subset \Omega_{\rho_{e_A}} \subset \Omega_{\rho_A}$, $\Omega_{\rho_{s_i}} \subset \Omega_{\rho_i}$, and:

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

$$\rho_i \geq \max\{V_i(x_i(t)) : x_i(t_k) \in \Omega_{\rho_{e_i}}, \forall t \subset [t_k, t_{k+1})\} \tag{9}$$

$$\rho_{\min,i} \geq \max\{V_i(x_i(t)) : x_i(t_k) \in \Omega_{\rho_{s,i}}, \forall t \in [t_k, t_{k+1})\} \tag{10}$$

where $i = A, 1, 2, \ldots$. If the initial state measurement satisfies $x_i(t_0) \in \Omega_{\rho_i}/\Omega_{\rho_{s,i}}$, $x(t) \in \Omega_{\rho_A}$ for all $t \geq 0$ when there are no attacks. Also, the profit under the proposed implementation strategy is no worse than that of the A-LMPC over a given sampling period.

Proof 1. The first part of the proof addresses feasibility of the A-LMPC and A-LEMPC, and whether a characterizable control action exists to be applied to the process at every sampling time despite that the i^{th} LMPC may be infeasible. The second part demonstrates that the closed-loop state remains within $\Omega_{\rho_A} \forall t \geq 0$ when no attacks occur. The third part demonstrates that, in the absence of cyberattacks, the profit over a given sampling period under the implementation strategy of Section 3.2 is no worse than under the A-LMPC over the same sampling period.

Part 1. To guarantee that a characterizable control action exists at each sampling time that can be applied to the process, we note that the i^{th} LMPC calculates the control action to be applied to the process, but it relies on the A-LMPC and A-LEMPC having been solved (to formulate the constraints of Eqs. 7g-7h). Thus, we first demonstrate that the A-LMPC and A-LEMPC are feasible at every sampling time so that the i^{th} LMPC can be formulated. To demonstrate feasibility of the A-LMPC, we note that under the conditions of the theorem, h_A applied in a sample-and-hold fashion throughout the prediction horizon is a feasible control action ($h_A(x(t_j))$, for $t \in [t_j, t_{j+1})$ where $j = k, \ldots, k+N-1$). This is because h_A trivially satisfies Eq. 5g, and satisfies Eq. 5d when $\tilde{x}(t) \in \Omega_{\rho_A} \subset X$, which is ensured under $h_A(x(t_j))$, $t \in [t_j, t_{j+1})$, $j = k, \ldots, k+N-1$, if $x(t_k) \in \Omega_\rho$ and the conditions of the theorem hold ($x(t) \in \Omega_{\rho_A}$, $\forall\ t \geq 0$, will be proven in *Part 2*). h_A satisfies Eq. 5e by Eq. 2d and trivially satisfies Eq. 5g (implemented at each sampling period in the prediction horizon) when Eqs. 8 and 10 hold.

Since the A-LMPC has a feasible solution, it will be able to generate the profit-related constraints of the A-LEMPC. Specifically, it will be used to generate the constraint of Eq. 6h. In that case, u^*_{al} (i.e., the optimal solution to the A-LMPC) is a feasible solution. This is because it satisfies the constraints of Eqs. 6b-6h (since Eqs. 6b-6e and 6g are also constraints of the A-LMPC and it satisfied them there, Eq. 6f will be satisfied by u^*_{al} if $x(t_k) \in \Omega_{\rho_{e_A}}$ for A-LMPC), and Eqs. 8 and 10 hold.

The i^{th} LMPC is not guaranteed to be feasible; however, the implementation strategy, in step 5, directs the use of the A-LMPC control action if the i^{th} LMPC is not feasible. Thus, the implementation strategy ensures that the A-LMPC and A-LEMPC have feasible solutions so that the i^{th} LMPC can be attempted to be solved, and if it is not feasible a characterizable control action will still be applied to the process that is guaranteed to be a feasible solution to the A-LMPC.

Part 2. To prove that $x(t) \in \Omega_{\rho_A}$ for all $t \geq 0$ when $x_i(t_0) \in \Omega_{\rho_i}/\Omega_{\rho_{s,i}}$, we note that from the implementation strategy of Section 3.2, one of two control actions will be applied: either the solution to the i^{th} LMPC (if it is feasible) or the control action computed by the A-LMPC. If the i^{th} LMPC is feasible at t_0, $\frac{\partial V_i(x_i(t))}{\partial x_i} f_i(x_i(t), u_i(t_k))$ is given by:

$$\begin{aligned}&\frac{\partial V_i(x_i(t))}{\partial x_i} f_i(x_i(t), u_i(t_0)) - \frac{\partial V_i(x_i(t_0))}{\partial x_i} f_i(x_i(t_0), u_i(t_0))\\ &+ \frac{\partial V_i(x_i(t_0))}{\partial x_i} f_i(x_i(t_0), u_i(t_0))\\ &\leq -\alpha_{3,i}(\alpha_{2,i}^{-1}(\rho_{s,i})) + L'_{x,i} M_{f,i}\Delta\end{aligned} \tag{11}$$

from Eqs. 7f, 2a, 2b, 3b, and 4. Thus, if Eq. 8 holds, V_i will decrease over a sampling period, keeping $x(t) \in \Omega_{\rho_A}$ for $t \in [t_0, t_1)$. A similar proof holds if instead $x(t_0) \in \Omega_{\rho_A}/\Omega_{\rho_{s_A}}$ and the i^{th} LMPC is not feasible at t_0. If the i^{th} LMPC is not feasible at t_0 but $x(t_0) \in \Omega_{\rho_{s_A}}$, Eq. 10 guarantees that $x(t) \in \Omega_{\rho_A}$, $t \in [t_0, t_1)$. Applying these results recursively (with Eq. 10 also guaranteeing that $x(t) \in \Omega_{\rho_A}$, $t \in [t_k, t_{k+1})$ in sampling periods where the i^{th} LMPC is feasible but $x_i(t_k) \in \Omega_{\rho_{s_i}}$), $x(t) \in \Omega_{\rho_A}$ at all times under the proposed implementation strategy.

Part 3. The economic performance under the implementation strategy with probing is at least as good as that of the stabilizing A-LMPC over any given sampling period. To show this, we note that the A-LEMPC enforces the constraint of Eq. 6h which forces the economically optimal A-LEMPC to perform as well as or better than its stabilizing counterpart (A-LMPC) over one sampling period. If the i^{th} LMPC is feasible, it computes a control action that provides a profit between that of the A-LMPC and the A-LEMPC through Eqs. 7g-7h. If it is not feasible, the control action computed by the A-LMPC is applied. Thus, in any given sampling period, the control action applied to the process will perform no worse than that of the A-LMPC, whether or not the i^{th} LMPC is feasible.

4. PROCESS EXAMPLE

In this section, we demonstrate the concept of finding a steady-state for the i^{th} LMPC from the A-LEMPC through a chemical process example involving a continuous stirred tank reactor (CSTR) from (Heidarinejad et al., 2012). The states of the system are the reactant concentration of species A, C_A, and the temperature in the reactor, T. The manipulated variables are the inlet concentration of reactant A (C_{A0}) and the rate of heat transferred to the system (Q). The state and input vectors are written in deviation variable form with respect to the process steady-state $[C_{As}\ T_s]^T = [1.22\ kmol/m^3\ 438.25\ K]^T$ (the steady-state process input is $[C_{A0s}\ Q_s]^T = [4.0\ \text{kmol/m}^3\ 0\ \text{kJ/h}]^T$). The Explicit Euler method is used to numerically integrate the process model by using an integration step of 10^{-4} h. The economic cost function to be maximized is $L_e = k_0 e^{-E/(RT)} C_A^2$ (rate of conversion of A). We design first an A-LMPC for the system with a prediction horizon of $N = 10$ and simulate the closed-loop state over one sampling period. For the design of the stability region and Lyapunov-based stability constraints, $V = x^T P x$, where

$P = [1200\,5;\ 5\,0.1]$, and $h(x) = [h_1(x)\ h_2(x)]^T$ has $h_1(x) \equiv 0$ kmol/m^3 and $h_2(x)$ is governed by Sontag's control law (Lin and Sontag, 1991). $\rho_A = 300$ and $\rho_{e,A} = 225$. The LEMPC optimization problems were solved in MATLAB R2023a using fmincon. The process was initialized at the state $x_{init} = [0.21\ \text{kmol/m}^3\ 28.92\ \text{K}]^T$ (in deviation variable form from the process steady-state). The constraint of Eq. 5g was only applied for the first sampling time in the prediction horizon (instead of at each sampling period in the prediction horizon). After one sampling period of operation under the A-LMPC, the process profit is 0.3858.

Next, the A-LEMPC is solved (though in this case, we do not impose a constraint on the profits as in Eq. 6h, but instead below will discuss the likelihood that such a constraint is feasible based on the profit results without this constraint). Unlike the A-LMPC, which computes control actions that decrease the value of the Lyapunov function over the sampling period, the A-LEMPC computes a value of the process input that increases the Lyapunov function value over the sampling period. This demonstrates that in general, the i^{th} LMPC attempting to track the trajectory of the A-LEMPC over a sampling period may take a very different trajectory from what would be taken by the A-LMPC. After one sampling period of operation under the A-LEMPC, the process profit is 0.4943. This is higher than the profit of the A-LMPC, indicating that we would expect the constraint of Eq. 6h to be feasible, despite that the parameters of this simulation example have not been rigorously selected to meet all theoretical requirements according to Theorem 1, suggesting that even heuristic implementations of the methodology presented in this work may still have opportunity to be solvable.

The state at the end of one sampling period under the A-LEMPC is at $C_A = 1.251$ kmol/m^3 and $T = 484.212$ K. This corresponds to steady-state inputs where the value of C_{A0} would be outside of the input bound for C_{A0} (the input bounds are $0.5 \le C_{A0} \le 7.5$ kmol/m^3 and $-5 \times 10^5 \le Q \le 5 \times 10^5$ kJ/h). One way of handling this would be to attempt to formulate the i^{th} LMPC with a different steady-state than $\tilde{x}(t_{k+1})$ computed by the A-LEMPC. For example, since the i^{th} LMPC of Eq. 7 is already not guaranteed to be feasible, another steady-state could be selected for which the corresponding steady-state input is within the input bounds, and the stability region for the new steady-state contains both the new steady-state and $x(t_k)$. The constraints of Eqs. 7g-7h could then still be applied. If they are infeasible, as in the case where the i^{th} steady-state came from the A-LEMPC, then the A-LMPC control action could be used instead. Thus, a benefit of the formulation of Eqs. 7g-7h (despite the potential infeasibility) is that the constraints which are not guaranteed to be feasible under h_i implemented in sample-and-hold (which are the profit constraints) serve as a sort of safe-guard for handling the issue from a profit perspective that the value of $\tilde{x}(t_{k+1})$ from the A-LEMPC was not guaranteed above to have the qualities required by step 5 of the implementation strategy in Section 3.2. Though one option if it does not would be to use the A-LMPC control action instead to ensure that the profit over the subsequent sampling period is at least as high as that of the A-LMPC, the two profit constraint in Eq. 7 also enable heuristic searching/guess-and-check for other potential steady-states that might improve profits over a sampling period compared to using the A-LMPC.

5. CONCLUSION

We demonstrated that three controllers can work together to, in the absence of disturbances, avoid profit loss due to active cyberattack probing over a sampling period.

REFERENCES

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

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

Heidarinejad, M., Liu, J., and Christofides, P.D. (2013). Algorithms for improved fixed-time performance of Lyapunov-based economic model predictive control of nonlinear systems. *Journal of Process Control*, 23(3), 404–414.

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

Mhaskar, P., El-Farra, N.H., and Christofides, P.D. (2006). Stabilization of nonlinear systems with state and control constraints using Lyapunov-based predictive control. *Systems & Control Letters*, 55(8), 650–659.

Narasimhan, S., El-Farra, N.H., and Ellis, M.J. (2022). Detectability-based controller design screening for processes under multiplicative cyberattacks. *AIChE Journal*, 68(1), e17430.

Oyama, H., Messina, D., Rangan, K.K., Leonard, A.F., Nieman, K., Durand, H., Tyrrell, K., Hinzman, K., and Williamson, M. (2023). Development of directed randomization for discussing a minimal security architecture. *Digital Chemical Engineering*, 6, 100065.

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

Rangan, K.K., Oyama, H., and Durand, H. (2022). Actuator cyberattack handling using Lyapunov-based economic model predictive control. *IFAC-PapersOnLine*, 55(7), 489–494.

Rawlings, J.B., Angeli, D., and Bates, C.N. (2012). Fundamentals of economic model predictive control. In *Proceedings of the Conference on Decision and Control*, 3851–3861. Maui, Hawaii.

Sánchez, H.S., Rotondo, D., Escobet, T., Puig, V., and Quevedo, J. (2019). Bibliographical review on cyber attacks from a control oriented perspective. *Annual Reviews in Control*, 48, 103–128.

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

Velarde, P., Maestre, J.M., Ishii, H., and Negenborn, R.R. (2017). Vulnerabilities in Lagrange-based DMPC in the context of cyber-security. In *2017 IEEE International Conference on Autonomic Computing (ICAC)*, 215–220.