Computers and Chemical Engineering 136 (2020) 106806

Contents lists available at ScienceDirect

Computers and Chemical Engineering

journal homepage: www.elsevier.com/locate/compchemeng

Cyber-attack detection and resilient operation of nonlinear processes under economic model predictive control

Scarlett Chen[a], Zhe Wu[a], Panagiotis D. Christofides[a,b,*]

[a] Department of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA, 90095-1592, USA
[b] Department of Electrical and Computer Engineering, University of California, Los Angeles, CA 90095-1592, USA

ARTICLE INFO

Article history:
Received 25 January 2020
Revised 3 March 2020
Accepted 3 March 2020
Available online 14 March 2020

Keywords:
Cyber-attacks
Attack detection
Neural networks
Process control
Model predictive control
Nonlinear processes

ABSTRACT

This work proposes resilient operation strategies for nonlinear processes that are vulnerable to targeted cyber-attacks, as well as detection and handling of standard types of cyber-attacks. Working with a general class of nonlinear systems, a modified Lyapunov-based Economic Model Predictive Controller (LEMPC) using combined closed-loop and open-loop control action implementation schemes is proposed to optimize economic benefits in a time-varying manner while maintaining closed-loop process stability. Although sensor measurements may be vulnerable to cyber-attacks, the proposed controller design and operation strategy ensure that the process will maintain stability and stay resilient against particular types of destabilizing cyber-attacks. Data-based cyber-attack detectors are developed using sensor data via machine-learning methods, and these detectors are periodically activated and applied online in the context of process operation. Using a continuously stirred tank reactor example, simulation results demonstrate the effectiveness of the resilient control strategy in maintaining stable and economically optimal operation in the presence of cyber-attacks. The detection results produced by the detection algorithm demonstrate the capability of the proposed method in identifying the presence of a cyber-attack, as well as in differentiating between different types of cyber-attacks. Upon successful detection of the cyber-attacks, the impact of cyber-attacks can be mitigated by replacing the attacked sensors by secure back-up sensors, and secure operation will resume with the process operated under the proposed resilient LEMPC control strategy.

1. Introduction

Cyber-physical systems (CPS) integrate communication networks, computation, and physical process components to ensure automated real-time operation in a seamless manner. Stable and secure operation of cyber-physical systems require accurate information and reliable communication technologies. In recent years, the cyber-security of cyber-physical systems has become increasingly important as more communication networks are replaced or complemented by wireless networks in addition to point-to-point communications (Christofides et al., 2007; Ahlén et al., 2019). While these new developments increase operation efficiency and performance, they also increase the system's vulnerability to cyber-attacks. Recent incidents of cyber-attacks on various industrial plants, such as the Iranian nuclear plant attack in 2010 and the Ukrainian electric power grid attack in 2015, demonstrated the capability of cyber-attacks in infiltrating CPS and the severity of their consequences. Malicious cyber-attacks could target any device or communication channels in the control network to modify control actions and jeopardize operational cost, stability, integrity, and other safety considerations. With access to technical details of the control system, these targeted cyber-attacks are intelligently designed to disrupt process operation and compromise fundamental process safety. As cyber-attacks pose severe threats to the control system, safety measures addressing cyber-security need to be carefully considered and incorporated in plant-wide risk assessments. A nonlinear systems framework for cyber-attack prevention was proposed in (Durand, 2018) to inspect cyber-attack-resilient properties of the process and of the control designs. The impact of cyber-attacks on critical infrastructures was assessed using methodologies in system dynamics and sensitivity analysis in Genge et al. (2015), and metrics were proposed for quantifying the propagation of cyber-attacks and significance of control variables.

On the other hand, with the increase in digital connectivity and computing power, potential applications of archived plant data could extend beyond day-to-day monitoring and operation. One example use of these "big data" approaches is cyber-attack and

* Corresponding author.
E-mail address: pdc@seas.ucla.edu (P.D. Christofides).

https://doi.org/10.1016/j.compchemeng.2020.106806
0098-1354/

anomaly detection. Due to the close interactions between cyber and physical components, operational cyber-security of control systems would mandate a different strategy than traditional information technology (IT) approaches – one that combines robust control strategies with an advanced detection scheme using the process data at hand, which can be found in Raiyn (2014).

Cyber-attacks can target actuators, sensors, communication channels between devices, and the control system algorithms; they modify the control implementation using process and control system information in an attempt to disrupt closed-loop performance. A comprehensive review in Ashibani and Mahmoud (2017) included analysis on security issues, requirements, and possible solutions at various layers of the CPS architecture. Moreover, a survey on cyber-physical systems security from the security perspective (taxonomy of threats, attacks, and controls), the cyber-physical components perspective, and from a holistic systems perspective was explored in Humayed et al. (2017), where representative systems such as smart grids, medical CPS, and smart cars were studied. A review of possible weaknesses in corporate networks, in the Supervisory Control and Data Acquisition (SCADA) and Distributed Control System (DCS) systems, and in production environments was presented in Asghar et al. (2019). Amongst sensor cyber-attacks, some common attack types are denial-of-service attacks, replay attacks, and deception attacks – such as min-max, geometric, and surge attacks (Cárdenas et al., 2011). For instance, for replay attacks commonly occurring on wireless sensor networks, a wormhole tunnel can be created between two end points to replay messages observed in different regions (Lee et al., 2014). The detection and control of replay attacks in smart grid systems specifically have also been studied in Tran et al. (2013); Zhao et al. (2016). Moreover, adversaries may launch other deception attacks through hacking remote terminal units (RTUs), such as sensors in substations in a power grid transmission system. In Amin et al., 2012, a hierarchical attack in automated canal systems was described with various deception attacks in different cyber layers, and a field-operational test attack was reported on the Gignac canal system located in Southern France. Due to the sophistication of cyber-attacks and their accessibility to control system information, they are intended to disrupt the closed-loop system while avoiding being detected by conventional detection methods or by control engineers, thus making them fundamentally different from sensor or actuator faults. Situations where conventional model-based detection schemes may be rendered ineffective by intelligent cyber-attacks can be potentially tackled by data-based detection methods (Cárdenas et al., 2011).

The development and applications of machine-learning methods in traditional engineering fields have increased in recent years, and more specifically in the field of systems engineering (Polycarpou and Ioannou, 1991; Rawlings and Maravelias, 2019; Wu et al., 2019; Venkatasubramanian, 2019). Machine learning techniques, such as artificial neural networks, support vector machines (Widodo and Yang, 2007), as well as more advanced deep learning methods, such as recurrent neural networks (Schuster and Paliwal, 1997; Hochreiter and Schmidhuber, 1997), have demonstrated effectiveness in plant anomaly detection (Samanta and Al-Balushi, 2003; Bishop, 2006; Singh and Nene, 2013). More specifically, the application of feed-forward artificial neural networks in modeling thin-film deposition processes (Chaffart and Ricardez-Sandoval, 2018; Kimaev and Ricardez-Sandoval, 2019) has provided comparable control performances, and the application of neural networks in detecting cyber-attacks in a chemical process has shown superior performance than traditional statistical methods in Wu et al. (2018). Motivated by this, machine-learning methodologies can be readily adopted in the context of control theory and cyber-physical security. In addition to having an adequate detection mechanism, control and operation strategies can be designed or adjusted accordingly if a process is vulnerable to cyber-attacks. Prior to developing control frameworks to address cyber-attacks in cyber-physical systems, there has been robust model-based control frameworks proposed to address uncertainties in the process. In Heidarinejad et al. (2012), it was assumed that the uncertain process variables were bounded, and the robustness of the controller was established with respect to the worst-case values of the uncertain variables such that the state of the closed-loop system stays within a well-characterized region of the state-space given that the uncertain variables are within sufficiently small bounds. Moreover, other tube-based model predictive controller approaches have been developed to achieve robustness against unstructured uncertainties (Mayne et al., 2011; Falugi and Mayne, 2013). In recent years, increasing research efforts have been dedicated to developing system and control designs to address cyber-attacks (Durand, 2018). For instance, novel methods and tools to support effective preliminary design efforts for new cyber-physical systems were presented in Carter et al. (2019), which addressed the integration of required defense and resilience solutions. A robust event-triggered model predictive control problem was investigated in Sun and Yang, 2019 when the process is subject to bounded disturbances and denial-of-service cyber-attacks. Cumulative Sum (CUSUM) detection method was used in Chamanbaz et al. (2019) in conjunction with model predictive control to operate a nonlinear system under false data injection attacks. Moreover, a robust two-tier control architecture was proposed in Chen et al. (2020) that provided convenient system reconfiguration strategies to maintain cyber-security. In light of these considerations, the contributions of this work are as follows: 1) A cyber-secure operation mode of economic model predictive control, 2) the construction of a data-based machine-learning detection algorithm, and 3) the application of the proposed operation and detection schemes to a benchmark nonlinear chemical process example. The remainder of this manuscript is organized as follows: The notation, the class of nonlinear process systems considered, as well as the formulation of Lyapunov-based economic model predictive control are shown in Section 2; the modified cyber-secure LEMPC formulations are presented in Section 3; the design of adapted intelligent cyber-attacks is shown in Section 4; the attack-resilient control strategies are developed in Section 5; the machine-learning-based detection algorithm is explained in Section 6; and the application of the proposed methodology to a nonlinear chemical process example is presented in Section 7.

2. Preliminaries

2.1. Nonlinear system formulation

In this work, $|\cdot|$ is used to denote the Euclidean norm of a vector; x^T denotes the transpose of x; $\mathbf{R}^{\mathbf{n}}_{+}$ denotes the set of vector functions of dimension n whose domain is $[0, \infty)$. Set subtraction is denoted by "\", i.e., $A \backslash B := \{x \in \mathbf{R}^n | x \in A, x \notin B\}$. Class $\mathcal{K}$ functions $\alpha(\cdot)$: $[0, a) \to [0, \infty]$ are defined as strictly increasing scalar functions with $\alpha(0) = 0$.

The class of continuous-time nonlinear systems considered is described by the following state-space form:

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

$$\bar{x}(t) = h(x(t)) \tag{1b}$$

where $x(t) \in \mathbf{R}^n$ is the state vector, and $u(t) \in \mathbf{R}^m$ is the manipulated input vector, which is constrained by $u \in U := \{u_i^{\min} \leq u_i \leq u_i^{\max}, i = 1, \ldots, m\} \subset \mathbf{R}^m$, where $u_i^{\min}$ and $u_i^{\max}$ are the lower and upper bounds for the input vector. We will denote the vector of state measurements from sensors, which may be compromised

by sensor cyber-attacks, with $\bar{x}(t) \in \mathbf{R}^n$. When no cyber-attacks are present in the system, $\bar{x}(t) = x(t)$. Without loss of generality, the initial time t_0 is taken to be zero ($t_0 = 0$). It is assumed that $f(\cdot)$ is a sufficiently smooth vector function of its arguments, and $h(\cdot)$ is a sufficiently smooth vector function of x where $f(0,0) = 0$, $h(0) = 0$. Thus, the origin is an equilibrium point of the system of Eq. 1 under $u(t) = 0$.

We assume that there exists an explicit feedback controller of the form $u(t) = \phi(x(t)) \in U$ that can render the origin of the nonlinear closed-loop system of Eq. 1 asymptotically stable.

The stabilizability assumption implies the existence of a positive definite control Lyapunov function $V(x)$ that satisfies the following conditions:

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

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

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

for all $x \in D \subseteq \mathbf{R}^n$, where D is an open neighborhood around the origin, and $\alpha_i(\cdot)$, $i = 1, 2, 3, 4$, are class $\mathcal{K}$ functions. Based on the universal Sontag control law (Lin and Sontag, 1991), a candidate controller $\phi(x)$ is given by the saturated control law accounting for the input constraint $u \in U$, which is shown as follows:

$$\varphi_i(x) = \begin{cases} -\dfrac{p + \sqrt{p^2 + |q|^4}}{|q|^2} q, & \text{if} \quad q \neq 0 \\ 0, & \text{if} \quad q = 0 \end{cases} \tag{3a}$$

$$\phi_i(x) = \begin{cases} u_i^{min}, & \text{if} \quad \varphi_i(x) < u_i^{min} \\ \varphi_i(x), & \text{if} \quad u_i^{min} \leq \varphi_i(x) \leq u_i^{max} \\ u_i^{max}, & \text{if} \quad \varphi_i(x) > u_i^{max} \end{cases} \tag{3b}$$

where p denotes $L_f V(x)$ and q denotes $(L_g V(x))^T = [L_{g_1} V(x) \cdots L_{g_m} V(x)]^T$. $\varphi_i(x)$ of Eq. 3a represents the i^{th} component of the control law $\phi(x)$ without considering saturation of the control action at the input bounds. $\phi_i(x)$ of Eq. 3b represents the i^{th} component of the saturated control law $\phi(x)$ that accounts for the input constraints $u \in U$.

We first characterize a set of states D, in which the time-derivative of the Lyapunov function $V(x)$ under $u = \phi(x) \in U$ is negative for $x \neq 0$. Then we construct a level set of $V(x)$ inside D as $\Omega_\rho := \{x \in D \,|\, V(x) \leq \rho,\ \rho > 0\}$, which represents an estimate of the stability region of the closed-loop system of Eq. 1, and Ω_ρ is an invariant set for the closed-loop system. Therefore, starting from any initial state $x_0 := x(t_0)$ in Ω_ρ, $\phi(x(t))$ guarantees that the state trajectory of the closed-loop system of Eq. 1 remains within Ω_ρ and asymptotically converges to the origin. Thus, given that the sensor measurements received by the controller are secure and reliable (i.e., $\bar{x}(t) = x(t)$), the control law $\phi(x(t))$ is able to stabilize the process at the origin for any initial conditions $x_0 \in \Omega_\rho$.

2.2. Lyapunov-based economic model predictive control

Within the traditional paradigm of process control, a two-layer architecture is utilized to increase process economic profits where the tracking model predictive control (MPC) is coupled with an optimizer referred to as a real-time optimizer (RTO) that computes economically optimal steady-states for the MPC to track by solving a nonlinear optimization problem with a detailed steady-state plant model and a possibly nonlinear and nonquadratic objective function representing the process economics.

However, as operational efficiency and increasing energy consumption are becoming critical issues in the chemical and petrochemical industry, a model-based feedback control strategy, economic model predictive control (EMPC), was proposed to operate the system off steady-state by dynamically optimizing an economic cost function while accounting for stability constraints. It has been repeatedly shown in the chemical process control literature that a number of industrially relevant processes can achieve higher profits when operated in a time-varying fashion than when operated at steady-state for all times; therefore, EMPC has been proposed as an efficient method to address process control problems integrated with dynamic economic optimization of the process (e.g., Amrit et al., 2011; Heidarinejad et al., 2012; Ellis et al., 2014).

Specifically, Lyapunov-based Economic Model Predictive Control (LEMPC) design is represented by the following optimization problem:

$$\mathcal{J} = \max_{u \in S(\Delta)} \int_{t_k}^{t_{k+N}} l_e(\tilde{x}(t), u(t)) dt \tag{4a}$$

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

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

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

$$V(\tilde{x}(t)) \leq \rho_e, \quad \forall\ t \in [t_k, t_{k+N}), \quad \text{if } \bar{x}(t_k) \in \Omega_{\rho_e} \tag{4e}$$

$$\dot{V}(\bar{x}(t_k), u) \leq \dot{V}(\bar{x}(t_k), \phi(\bar{x}(t_k))), \quad \text{if } \bar{x}(t_k) \in \Omega_\rho \backslash \Omega_{\rho_e} \tag{4f}$$

where $\tilde{x}$ is the predicted state trajectory, $S(\Delta)$ is the set of piecewise constant functions with period Δ, and N is the number of sampling periods in the prediction horizon. $\dot{V}(x, u)$ is used to represent $\frac{\partial V(x)}{\partial x} f(x, u)$. The optimal input trajectory computed by the EMPC is denoted by $u^*(t)$, which is calculated over the entire prediction horizon $t \in [t_k,\ t_{k+N})$. The control action computed for the first sampling period of the prediction horizon $u^*(t_k)$ is sent by the EMPC to be applied over the next sampling period in a sample-and-hold manner, and the EMPC is solved again in a rolling horizon fashion. The EMPC of Eq. 4 is solved by optimizing the time integral of the cost function $l_e(\tilde{x}(t), u(t))$ of Eq. 4a that accounts for process economic benefits over the prediction horizon subject to the constraints of Eqs. 4b–4f. Eq. 4c defines the input constraints applied over the entire prediction horizon. Eq. 4d defines the initial condition $\tilde{x}(t_k)$ of Eq. 4b, which is the state measurement $\bar{x}(t)$ at $t = t_k$. The constraint of Eq. 4e maintains the closed-loop state predicted by Eq. 4b in Ω_{ρ_e} over the prediction horizon if the state $\bar{x}(t_k)$ is inside Ω_{ρ_e}, where Ω_{ρ_e} is a conservative region within the closed-loop stability region Ω_ρ to make it an invariant set in the presence of sufficiently small bounded disturbances. However, if $\bar{x}(t_k)$ leaves Ω_{ρ_e} but still remains in Ω_ρ, the contractive constraint of Eq. 4f drives the state towards the origin for the next sampling period such that the state will eventually enter Ω_{ρ_e} within finite sampling periods. Therefore, under the LEMPC of Eq. 4, the closed-loop state is maintained within the closed-loop stability region Ω_ρ for all times while optimal economic profits can be achieved via time-varying operation. The closed-loop stability proof can be found in Ellis et al. (2014).

3. Cyber-secure LEMPC operation strategies

Given that EMPC operates the system in an off steady-state manner, cyber-attacks that target EMPC systems can be designed to

compromise both closed-loop stability and process economic benefits. Specifically, similar to the cyber-attacks that have been designed for tracking MPC (Wu et al., 2018), cyber-attacks for EMPC systems can be designed to drive states out of the stability region as fast as possible (e.g., min-max cyber-attack). The EMPC receiving falsified state measurements will compute incorrect control actions that will eventually cause the true process states to exit the stability region. The unstable evolution of state trajectory may occur even sooner in a system operated under EMPC than under tracking MPC since the system is operated off steady-state. Therefore, the selection of operating region, design of operating strategies, and integration of detection schemes need to be carefully considered.

3.1. Operation within secure operating region

Considering that sensors are vulnerable to cyber-attacks, the process will be operated within a smaller region, $\Omega_{\rho_{secure}}$, where $0 < \rho_{secure} < \rho_e$, to avoid the system from immediately losing stability when under malicious cyber-attacks.

Although economic benefits will not be maximized when operated based on $\Omega_{\rho_{secure}}$ compared to operation around the original region Ω_{ρ_e}, it allows the system leeway to detect and mitigate the cyber-attack before closed-loop stability is lost (i.e., before true process states $x(t)$ exit Ω_ρ). The goal of detection is to identify the occurrence of a cyber-attack before the true process states exit the closed-loop stability region Ω_ρ, such that the process can be eventually driven back to and stay bounded within the secure region $\Omega_{\rho_{secure}}$ under LEMPC after eliminating the impact of cyber-attacks. The modified LEMPC formulation is presented as follows:

$$\mathcal{J} = \max_{u\in S(\Delta)} \int_{t_k}^{t_{k+N}} l_e(\tilde{x}(t), u(t))dt \tag{5a}$$

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

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

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

$$V(\tilde{x}(t)) \le \rho_{secure}, \quad \forall\ t \in [t_k, t_{k+N}), \quad \text{if } \bar{x}(t_k) \in \Omega_{\rho_{secure}} \tag{5e}$$

$$\dot{V}(\bar{x}(t_k), u) \le \dot{V}(\bar{x}(t_k), \phi(\bar{x}(t_k))), \quad \text{if } \bar{x}(t_k) \in \Omega_\rho \backslash \Omega_{\rho_{secure}} \tag{5f}$$

where the notations follow those in Eq. 4. The constraint of Eq. 5e maintains the closed-loop states within $\Omega_{\rho_{secure}}$ over the prediction horizon if current state $\bar{x}(t_k)$ is inside $\Omega_{\rho_{secure}}$, and the contractive constraint of Eq. 5f will be activated when process states are outside of the neighborhood $\Omega_{\rho_{secure}}$. Since $\Omega_{\rho_{secure}}$ is characterized as a subset of Ω_{ρ_e} (i.e., $\rho_{secure} < \rho_e < \rho$), when the process state vector $\bar{x}(t_k)$ is inside $\Omega_{\rho_{secure}}$, it is guaranteed that under sufficiently small bounded disturbances $x(t_{k+1})$ will not exit Ω_ρ. Therefore, Ω_{ρ_e} is determined accounting for bounded disturbances and sample-and-hold implementation of control actions to ensure the invariance of Ω_ρ. In the presence of bounded disturbances, Ω_{ρ_e} can be found computationally (Heidarinejad et al., 2012).

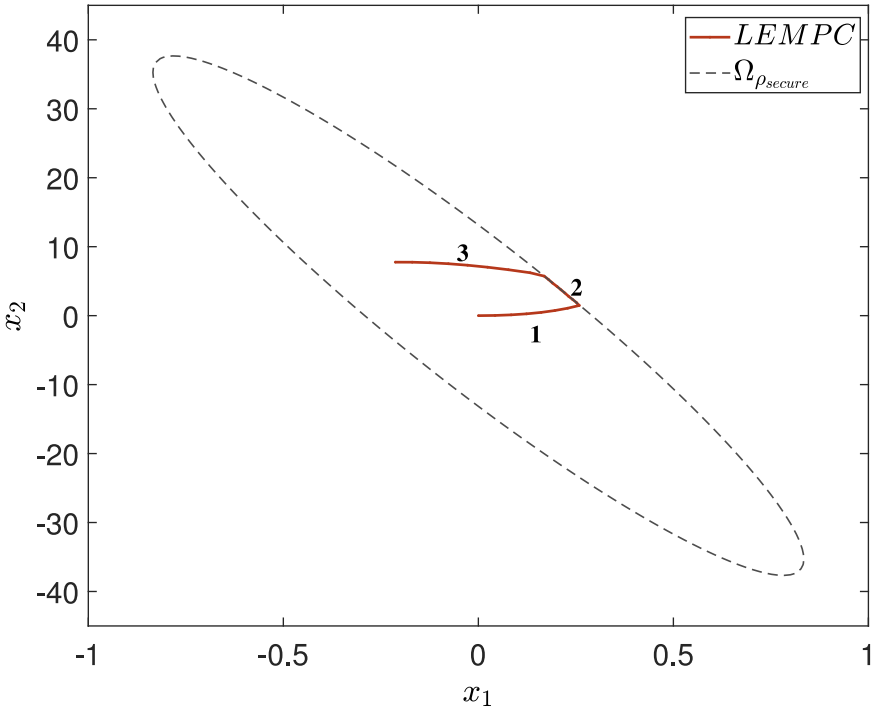
Furthermore, it is common that chemical processes are subject to periodic feed stock constraints, which are specified as part of the input constraint set U, where the quantity of feed materials is limited within a fixed period of time t_{N_p}. During this period of time, the total feed material is constrained to a constant value C, i.e., $\frac{1}{t_{N_p}} \int_{t_0}^{t_{N_p}} u_m(\tau)d\tau = C$, where u_m represents feed material used at every sampling period. Therefore, the material consumption constraint renews every t_{N_p}. If the total operation time is longer than one material constraint period, this material consumption constraint results in cyclic operation of the plant, and consequently, cyclic behavior of the state-space trajectory. At the start of a new material constraint period, the total consumption limit is renewed, as new feed materials become available to be used again for the next constraint period.

Fig. 1 illustrates the trajectories of the states and the input constrained by feed materials under normal operation of LEMPC over one material constraint period. Assuming the process starts from the operating steady-state (e.g., the origin), since EMPC maximizes the economic benefits while maintaining closed-loop stability during operation, it will drive the process states in the direction where economic benefit is optimized using large inputs until process states reach the boundary of the secure region $\Omega_{\rho_{secure}}$, as shown in Segment 1 in Fig. 1. Following this, the optimized state trajectory will progress along the boundary of $\Omega_{\rho_{secure}}$, as illustrated in Segment 2 in Fig. 1. Process states will remain on the boundary until the input materials start to exhaust and the input consumption constraints start restricting process states from further progressing along the boundary. With restricted inputs, the process states will be driven away from operating on the boundary – this is shown in Segment 3 in Fig. 1.

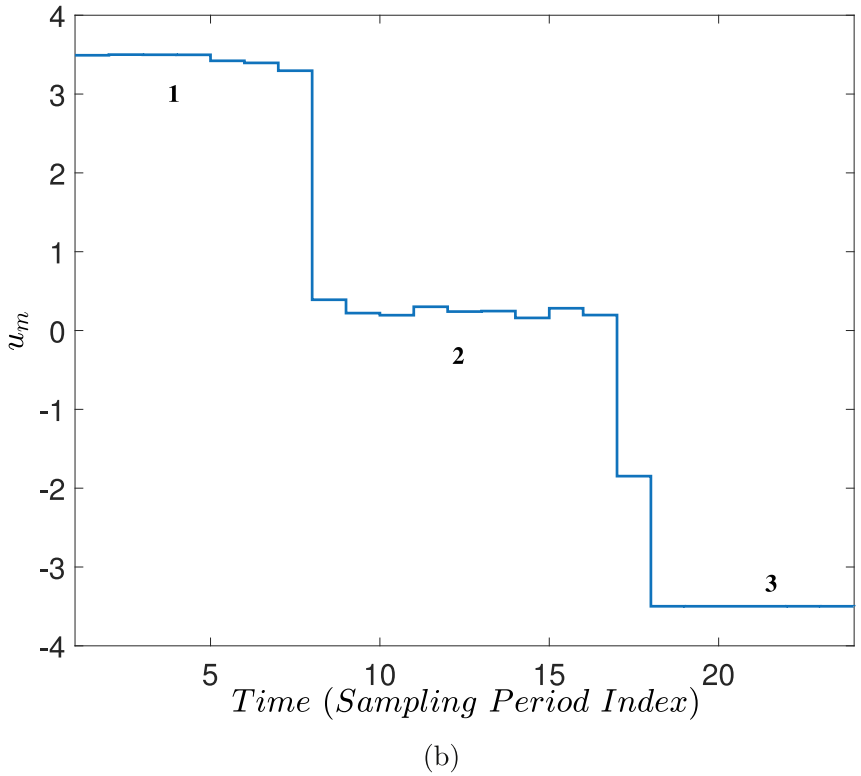
Remark 1. Additionally, stealthy cyber-attacks can be designed with the aim of decreasing process economic benefits by driving the true process state to the region with low economic profits (but still within the closed-loop stability region). Since cyber-attacks targeting process economic profits will not cause physical damage or accidents, they are more difficult for process engineers to detect. Under the assumption that attackers know the process model and the stability region, such cyber-attacks will compromise sensor measurements such that the control actions calculated by the optimization problem of EMPC will not increase process economic profits for the next sampling period as much as it would do under nominal operation. In this study, we only consider attacks that intend to compromise process stability.

4. Intelligent cyber-attacks

Intelligent cyber-attacks are designed to intentionally destroy the control objectives of the system, disrupting system stability and degrading control performance. Cyber-attacks could compromise sensors, actuators, and/or the communication channels between them. In this work, we only consider attacks on sensor measurements. Sensor feedback measurements must accurately report the true state of the process to ensure closed-loop stability; falsified measurements may result in control actions that will no longer achieve maximum economic benefit and may ultimately drive the true process states outside of the stability region. There are some standard types of cyber-attacks considered in literature (Singh and Nene, 2013). Min-max cyber-attacks aim to achieve maximum disruptive impact within shortest amount of time. Surge attacks cause maximum deviation for an initial “surge” period, and then the attacked value is set to a reduced value for the remainder of the attack duration such that the cumulative deviation will not exceed a certain threshold that will trigger alarms in conventional detection methods such as Cumulative Sum (Mohanty et al., 2007; Cárdenas et al., 2011). Geometric attacks geometrically increase the deviation of the attacked value from its true value until it reaches the alarming threshold. Details on the formulations of the four attack types can be found in Section 4.1. Being process and controller behavior aware, the cyber-attacks will have access to information on the operating region of the process under LEMPC $\Omega_{\rho_{secure}}$, and existing alarms configured on the input and output ranges. Specifically, when attacks intend to induce maximum disruption (i.e., in



(a)



(b)

Fig. 1. Trajectories of (a) process states x_1 and x_2, and (b) manipulated input u_m, under normal LEMPC operation over one material constraint period.

min-max or surge attacks), the attacked value will be set to the maximum or minimum value beyond which an alarm monitoring the current state measurement will be immediately triggered. These intelligent cyber-attacks are designed such that no alarms will be sounded (i.e., the falsified state measurement is not outside the operating stability region or the alarm window) and the controller is still able to compute feasible control actions, but have large enough variations such that economic optimality and closed-loop stability will be lost.

To train a machine-learning-based detector, closed-loop data will be collected where attacks with varying durations L_a are introduced at random times i_0 during the simulation period. If no

attacks occur within the simulation period (or the detection window), then the measurement signals are classified as "no attack". Furthermore, we consider a system where some sensors are attacked and some remain intact. For clarity, only one type of cyber-attack will occur at a time during the simulation period.

4.1. Design of cyber-attacks adapted to secure LEMPC operation

The system is now operated under the modified LEMPC of Eq. 5, where the operating region is set to be a smaller level set of $V(x)$, $\Omega_{\rho_{secure}}$, within the stability region, where $0 < \rho_{secure} < \rho_e < \rho$. Thus, the cyber-attacks imposed on the sensors also need to be adapted to prevent having a falsified measurement beyond the operating region $\Omega_{\rho_{secure}}$ and to avoid triggering any immediate alarms based on the values of the state measurements. The adapted mathematical formulations of min-max, surge, geometric, and replay attacks are presented in the following sections.

4.1.1. Min-Max cyber-attack

While avoiding triggering any alarms, min-max attacks result in maximum destabilizing impact within a short time period. Therefore, the falsified state measurements take values that are furthest from the equilibrium point (minimum or maximum) but not outside of the secure operating region $\Omega_{\rho_{secure}}$.

The min-max attack can be formulated as follows:

$$\bar{x}(t_i) = \arg\min / \max_{x \in \mathbf{R^n}} \{V(x(t_i)) \leq \rho_{secure}\}, \quad \forall\ i \in [i_0, i_0 + L_a] \tag{6}$$

where ρ_{secure} defines the level set of the Lyapunov function $V(x)$ that characterizes the secure operating region of the closed-loop system of Eq. 1 under LEMPC, $\bar{x}$ is the compromised sensor measurement, i_0 is the time instant that the attack is introduced, and L_a is the total duration of the attack in terms of sampling periods.

4.1.2. Surge cyber-attack

Surge attacks maximize the disruptive impact for an initial short period of time, then they remain at a lower value for the rest of the attack duration. The maximum or minimum attack value is also defined based on the secure operating region, $\Omega_{\rho_{secure}}$. The length of the initial surge period and the reduced value after the surge can be designed in many ways as long as the cumulative error from t_{i_0} to $t_{i_0+L_a}$ between state measurements and their predicted true values does not exceed the threshold defined in some statistic-based detection methods (e.g., CUSUM). In our study, the reduced value after the surge is set to act as a sufficiently small bounded noise imposed on the attacked sensor. The formulation of the surge attack is presented below:

$$\begin{aligned} \bar{x}(t_i) &= \arg\min / \max_{x \in \mathbf{R^n}} \{V(x(t_i)) \leq \rho_{secure}\}, \quad \text{if } i_0 \leq i \leq i_0 + L_s \\ \bar{x}(t_i) &= x(t_i) + \eta(t_i), \quad \text{if } i_0 + L_s < i \leq i_0 + L_a \end{aligned} \tag{7}$$

where i_0 is the start time of the attack, L_s is the duration of the initial surge, and $\eta_l \leq \eta(t_u) \leq \eta_u$ is the bounded noise added on the sensor measurement after the initial surge period, where η_l and η_u are the lower and upper bounds of the noise, respectively.

4.1.3. Geometric cyber-attack

Under geometric cyber-attacks, closed-loop system stability deteriorates at a geometric speed until the cyber-attack reaches the maximum or minimum allowable value as characterized by the secure operating region. At the start of the attack t_{i_0}, a small constant $\beta \in \mathbf{R}$ is added to the true measured output $x(t_{i_0})$, where $x(t_{i_0}) + \beta$ is well below the alarm threshold. Following that, at each subsequent time step, β is multiplied by a factor $(1+\alpha)$, where $\alpha \in (0, 1)$, until $\bar{x}$ reaches the maximum allowable attack value bounded by $\Omega_{\rho_{secure}}$. Thus, attackers will choose the two parameters α and β based on $\Omega_{\rho_{secure}}$ and the attack duration. Geometric attacks can be written in the form as follows:

$$\bar{x}(t_i) = x(t_i) + \beta \times (1+\alpha)^{i-i_0}, \quad \forall\ i \in [i_0, i_0 + L_a] \tag{8}$$

where β and α are parameters that define the magnitude and speed of the geometric attack.

4.1.4. Replay cyber-attack

Replay cyber-attacks have access to all previous system outputs corresponding to secure nominal operating conditions where no cyber-attacks are present. The attacker extracts segments of these previous state measurements and injects them into the current measurement readings. As the replayed values are given by secure sensors and supposedly inside the secure operating bounds, classical detectors will not be able to recognize any abnormalities. Replay attacks can be represented by the following equations:

$$\bar{x}(t_i) = x(t_k), \quad \forall\ k \in [k_0, k_0 + L_a], \quad \forall\ i \in [i_0, i_0 + L_a] \tag{9}$$

where $x(t_k)$ is the true plant measurement, L_a represents the length of the attack (which is also the length of the replay segment) in terms of sampling periods, and $\bar{x}$ is the series of replay attacks added at time t_{i_0} duplicating previous state measurements that are recorded starting from time t_{k_0}. The duration of the attack could be exactly the length of one or more material constraint periods. Therefore, the tampered state trajectory would look identical to the nominal state trajectory of one (or more) complete cycle(s) of operation starting from a different set of initial conditions.

5. Attack-resilient combined open-loop and closed-loop control

Due to the LEMPC constraints of Eqs. 5e and 5f, for any initial condition $x_0 \in \Omega_\rho$, the evolution of state trajectory $x(t)$ will be driven towards but ultimately bounded inside the secure region $\Omega_{\rho_{secure}}$. As the economic benefit of the process is maximized with respect to the state vector, it is likely that during one material constraint period, the optimized states will reach, and evolve along the boundary of the secure region $\Omega_{\rho_{secure}}$, which is a level set of the control Lyapunov function $V(x)$. Assuming that the attacker has knowledge on the stability region as well as the secure region that the LEMPC operates based on, in order to induce maximum destructive impact on the system (e.g., in a min-max or surge cyber-attack) without triggering any alarms, the tampered state measurements will be near or on the boundary of the secure region $\Omega_{\rho_{secure}}$. Therefore, regardless of the presence of a cyber-attack, the measured process states will likely reach the boundary of $\Omega_{\rho_{secure}}$ where $V(\bar{x}) = \rho_{secure}$ during the operation of one material constraint period. In other words, when measured process states yield $V(\bar{x}) = \rho_{secure}$, there could be two reasons: 1) Following optimized control actions $u^*(t_k)$, the measured process states reach the boundary of the bounded secure region $\Omega_{\rho_{secure}}$ at time t_k under the normal operation with no cyber-attacks, or 2) the measured states are compromised by a cyber-attack (e.g., min-max, or surge) at time t_k. Therefore, when measured states $\bar{x}(t_k)$ provide $V(\bar{x}(t_k)) = \rho_{secure}$, this measurement can no longer be trusted due to the ambiguous cause of this observation, and closed-loop control can no longer be carried out.

To combat the ambiguity of state measurements when they are on the boundary of $\Omega_{\rho_{secure}}$, open-loop control actions will be used in conjunction with closed-loop control. Assuming that the states measured at the beginning of each material constraint period, $t = t_{N_0}$, (or initial conditions at $t = t_0$) are secure and correct, the open-loop control actions are computed at the beginning of the material constraint period by solving the following nonlinear optimization problem:

$$\mathcal{J} = \max_{u' \in S(\Delta)} \int_{t_{N_0}}^{t_{N_0+N_p}} l_e(\tilde{x}(t), u'(t))dt \tag{10a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}(t) = f(\tilde{x}(t), u(t)) \tag{10b}$$

$$u'(t) \in U, \quad \forall\ t \in [t_{N_0}, t_{N_0+N_p}) \tag{10c}$$

$$\tilde{x}(t_{N_0}) = \bar{x}(t_{N_0}) \tag{10d}$$

$$V(\tilde{x}(t)) \leq \rho_{secure}, \quad \forall\ t \in [t_{N_0}, t_{N_0+N_p}), \quad \text{if } \bar{x}(t_{N_0}) \in \Omega_{\rho_{secure}} \tag{10e}$$

$$\dot{V}(\bar{x}(t_{N_0}), u) \leq \dot{V}(\bar{x}(t_{N_0}), \phi(\bar{x}(t_{N_0}))), \quad \text{if } \bar{x}(t_{N_0}) \in \Omega_\rho \backslash \Omega_{\rho_{secure}} \tag{10f}$$

where N_p is the number of sampling periods in one material constraint period, which is the prediction horizon for open-loop control. When a new material constraint period begins, the EMPC in open-loop control mode receives state measurement and computes the optimal trajectory of N_p control actions that will be applied in a sample-and-hold manner until the end of this material constraint period. In the case that there are no cyber-attacks or process disturbances, this optimal trajectory of control actions would yield maximum economic benefits while meeting all input and state constraints.

While at closed-loop operation, if feedback measurement is no longer reliable and cannot be used for closed-loop control, the open-loop control actions that were calculated at the beginning of the material constraint period will be used as a substitute until the end of the material constraint period. At the end of the material constraint period, a cyber-attack detector is activated to determine any occurrence of an attack, and the reliability of the control system is re-assessed. The detector will provide information on the security status of the feedback measurements over the latest material constraint period. Upon mitigating the impact of a confirmed attack and/or confirming the security of the control system, closed-loop control with secure feedback measurement can be reactivated as a new material constraint period starts.

Although the absence of feedback may result in minor performance degradation in the case that process disturbances and modeling error exists and no cyber-attack is present, this strategy also completely eliminates the impact of a min-max or surge attack on the sensor measurements. The implementation strategy is illustrated in a logic flow diagram in Fig. 2, and the specific steps are outlined as follows:

1. At the start of a material constraint period ($t = t_{N_0}$), open-loop control actions over the course of the material constraint period are computed following Eq. 10. Closed-loop control is active, calculating the optimal control action over the next sampling period following Eq. 5.
2. If $\rho_{secure} - V(\tilde{x}(t_k)) \leq c$, (where $c > 0$ quantifies the distance from the boundary of secure region to categorize a state measurement as being untrustworthy), then closed-loop control (i.e., the modified LEMPC of Eq. 5) will be deactivated and open-loop control action $u'(t_k)$ calculated by the LEMPC of Eq. 10 will be used as an substitute.
3. Open-loop control actions $u'(t_k)$ will be used until $t_{N_0+N_p}$.

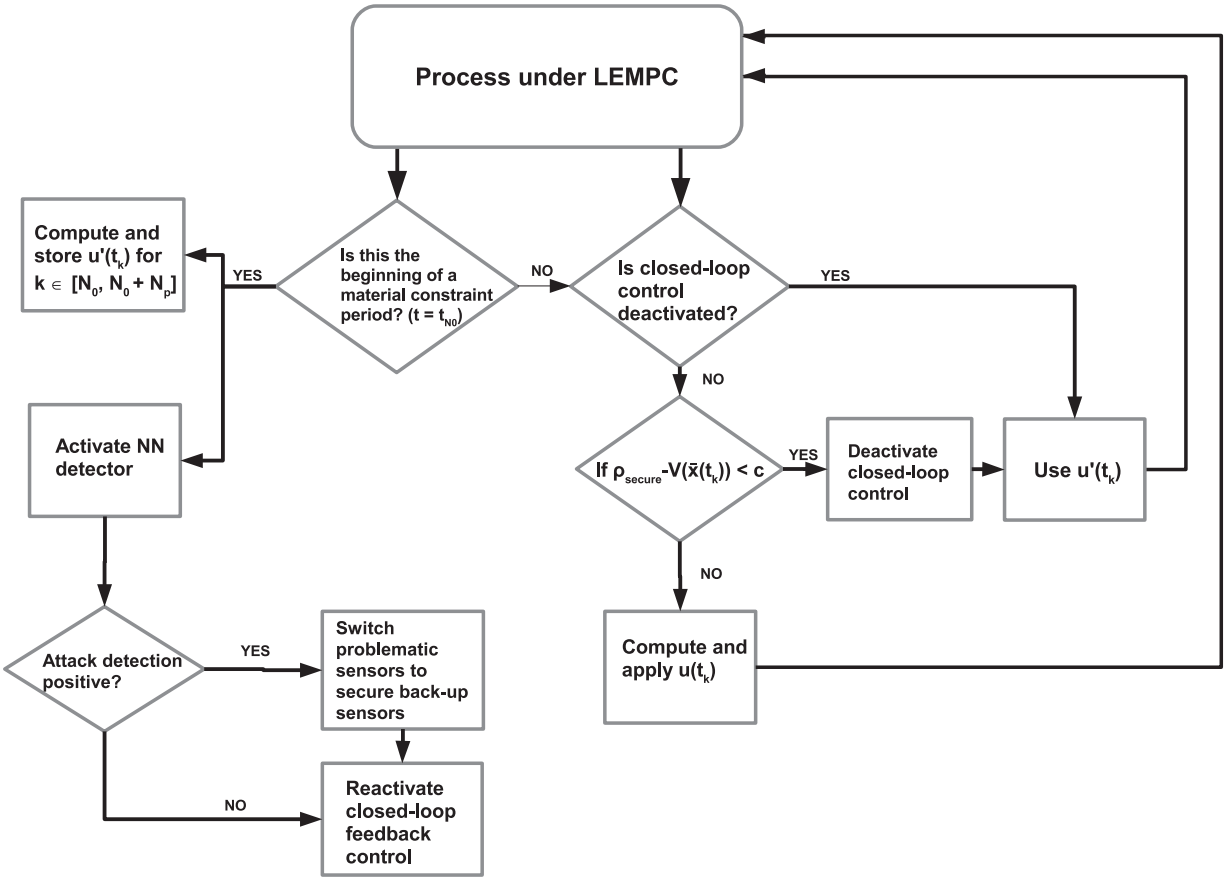


Fig. 2. Logic flowchart outlining the implementation steps of the attack-resilient operation of LEMPC using combined closed-loop and open-loop control actions when operating within a secure region $\Omega_{\rho_{secure}}$.

4. At $t_{N_0+N_p}$, the cyber-attack detector is activated to examine past full-state measurements $\bar{x}(t_k)$ for $k \in [N_0, N_0 + N_p]$. If an attack is detected, then disconnect the tampered sensors, reroute these measurement signals to a set of secure back-up sensors, and go to Step 5. If detection indicates no attack, go to Step 5.
5. At $t_{N_0+N_p}$, a new material constraint period starts, and closed-loop control is reactivated. Repeat Steps 1 – 4.

Remark 2. In some cases, the system may never reach the boundary of $\Omega_{\rho_{secure}}$ depending on the initial condition, the size of $\Omega_{\rho_{secure}}$, and the length of the material constraint period. If this is the case, and cyber-attacks wrongfully set the measured states to be on the boundary of $\Omega_{\rho_{secure}}$, then closed-loop control will still be deactivated following the implementation of Step 2, and open-loop control actions will be used.

Remark 3. In our study, we do not consider systems under large disturbances. Since open-loop control actions over the entire operating period are calculated by LEMPC at the beginning of the simulation period based on the nominal system, closed-loop stability is guaranteed using open-loop control if there are no disturbances or model uncertainties in the real process given that the process is open-loop stable. In the presence of process disturbances other than cyber-attacks, estimations of true process states are needed and closed-loop control can be applied based on these estimated states to stabilize the system within a bounded region. However, in our manuscript, we assume that the actual nonlinear process is disturbance-free; therefore, open-loop control is able to ensure closed-loop stability until the end of the material constraint period (i.e., the time instant at which NN detection will be activated and closed-loop control will resume).

6. Detection of cyber-attacks targeting EMPC

Cyber-attack detection carried out using data-based approaches, and more specifically, machine-learning methods, have been studied in many literature (Huang et al., 2007; Omar et al., 2013; Agrawal and Agrawal, 2015). Using data-based methods to train a detection algorithm for cyber-attacks separates the detector from the physical process model, and therefore makes the detector resilient to both process changes and intelligent stealthy attacks designed based on process behavior.

Amongst advanced machine-learning methods, neural networks (NN) have been successful in a wide range of applications for both supervised and unsupervised classifications (Gurney, 2014). There are also other types of state-of-the-art machine-learning classification methods that have been used in a variety of applications in recent literature, such as k-nearest-neighbors, random forest, and support vector machine (Hassan et al., 2018). Amongst these machine-learning algorithms, the advantage of neural network is that it provides a broad class of tuning parameters and a variety of nonlinear activation functions to optimize the overall model. Furthermore, neural networks can be developed using multiple different training algorithms, providing more alternatives during training to obtain better performance results (Tu, 1996). In a supervised classification problem, by training the neural network with labeled data corresponding to each target class, the neural network can be used to classify new data into classes that share similar characteristics. Depending on the training data, the neural network can distinguish between two (i.e., “attack” or “no attack”) or multiple classes (each class representing a known type of attack).

We use a feed-forward artificial neural network for supervised classification in our study. Each layer in the neural network consists of a series of nonlinear functions, yielding values for the neurons in the subsequent layer from the previous layer. Specifically, the neurons in the first hidden layer are derived from the inputs, and the neurons in the output layer are calculated from those in the last hidden layer. These nonlinear functions are activation functions of the weighted sum of inputs (or neurons in the previous layer) with an added bias term.

The structure of a basic neural network model employed here is shown in Fig. 3, with each input representing a nonlinear function $p(\cdot)$ of the full state measurements at each sampling time, and an output vector for predicted class label. The mathematical formulation of a two-hidden-layer feed-forward neural network is as follows:

$$\theta_j^{(1)} = g_1\left(\sum_{i=1}^{N_T} w_{ij}^{(1)} p(\bar{x}(t_i)) + b_j^{(1)}\right) \tag{11a}$$

$$\theta_j^{(2)} = g_2\left(\sum_{i=1}^{h_1} w_{ij}^{(2)} \theta_i^{(1)} + b_j^{(2)}\right) \tag{11b}$$

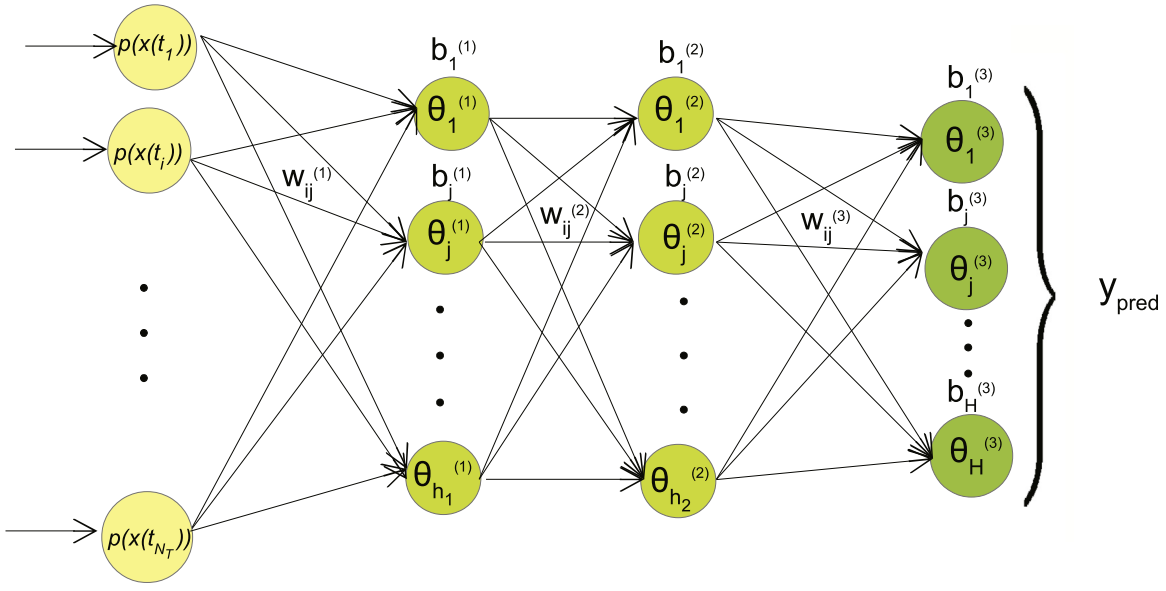


Fig. 3. Feed-forward neural network structure with 2 hidden layers with inputs being a nonlinear function $p(\bar{x})$ at each sampling time of the model predictive controller within the detection window N_T, and output being the probability of each class label for the examined trajectory indicating the status and/or type of cyber-attack.

$$\theta_j^{(3)} = g_3\left(\sum_{i=1}^{h_2} w_{ij}^{(3)}\theta_i^{(2)} + b_j^{(3)}\right), \quad y_{pred} = [\theta_1^{(3)}, \theta_2^{(3)}, \ldots, \theta_H^{(3)}]^T \quad (11c)$$

with $\theta_j^{(1)}$ and $\theta_j^{(2)}$ representing neurons in the first and second hidden layer, respectively, where $j = 1, \ldots, h_l$ is the number of neurons in layer $l = 1$ and $l = 2$. $\theta_j^{(3)}$ represents neurons in the output layer ($l = 3$), where $j = 1, \ldots, H$, and H is the number of class labels. In this study, we use two hidden layers for the cyber-attack detector design; however, multiple hidden layers can also be developed using similar formulations. For each sample, the input layer consists of variables $p(\bar{x}(t_i))$, which is a nonlinear function of the full-state measurements at time t_i, where $i = 1, \ldots, N_T$ is the length of the time-varying trajectory. The weights connecting neurons i and j in consecutive layers (from $l-1$ to l) are $w_{ij}^{(l)}$, and the bias term on the j^{th} neuron in the l^{th} layer is $b_j^{(l)}$. Each layer calculates an output based on the information received from the previous layer, as well as the optimized weights, biases, and the nonlinear activation function g_l (some examples include hyperbolic tangent sigmoid transfer function $g(z) = \frac{2}{1+e^{-2z}} - 1$, and softmax function $g(z_j) = \frac{e^{z_j}}{\sum_{i=1}^{H} e^{z_i}}$ where H is the number of class labels). Various common activation functions including ReLu, sigmoid, radial basis functions were presented and their performances were analyzed in Sibi et al. (2013). Furthermore, while Bayesian regularization is a powerful regularization method to avoid over-fitting and over-training, there are also other regularization algorithms such as L2 and L1 regularization, both of which add a parameter penalty in the objective function in an effort to reduce the generalization error (thus, the testing error) of the trained model. The advantage of Bayesian regularization is that it provides a probability distribution of optimal parameters instead of a single optimal value, thereby effectively dropping out trivial nodes to speed up the training process. In the output layer, y_{pred} is a vector giving the predicted probabilities of each class label. The predicted class label for the examined sample is indicated by the neuron with the highest probability, which in turn provides information on either the presence of a cyber-attack, or the type of the cyber-attack, depending on the classification problem the neural network is trained to solve.

To obtain an optimal set of weights and biases in Eq. 11, the Levenberg–Marquardt algorithm (Gavin, 2019) is used to minimize a Bayesian regularized mean squared error cost function, which has the following form:

$$S(w) = \gamma \sum_{k=1}^{N_s} (y_{pred,k} - y_{true,k})^2 + \zeta \sum_{p=1}^{N_w} w_p^2 \quad (12)$$

where $k = 1, \ldots, N_s$ represents the number of samples in the training dataset, $p = 1, \ldots, N_w$ represents the number of weights and biases in the neural network, y_{true} is the vector of target class labels of each sample, y_{pred} is the vector of the predicted probabilities associated with each class label, and γ and ζ are the regularization hyper-parameters. Within the Levenberg–Marquardt algorithm, the gradient and the Hessian matrix of $S(w)$ are calculated using the backpropagation method. The weights and the data are assumed to have Gaussian prior probability distributions. Then, the regularization hyper-parameters, γ and ζ, are updated by maximizing their posterior probability distribution provided the data, which is equivalent to maximizing the likelihood of evidence by Bayes' Theorem. Within each epoch, two sequential procedures are carried out: the cost function $S(w)$ is minimized with respect to w, and the likelihood of evidence is maximized with respect to γ and ζ. Detailed formulation of this procedure can be found in Burden and Winkler (2008). Training and testing accuracies are calculated, which are the ratios between the number of correctly classified samples and total number of samples in the training and testing sets, respectively.

To develop an NN detector, state measurement data are collected while the system is operated under the modified LEMPC of Eq. 5. For better detection accuracy, various state evolutions within the stability region under different operating conditions need to be accounted for; therefore, training data is collected for a broad range of initial conditions within the stability region Ω_ρ. Full state measurements $\bar{x}(t)$ are recorded along the time-varying trajectory for $t \in [t_0, t_{N_T}]$, and a nonlinear function denoted by $p(\bar{x})$ is computed. In order to provide an effective one-dimensional input feature for the detection problem, the function $p(\bar{x})$ needs to capture the dynamic behavior of all states. The selection of this input variable, $p(\bar{x})$, is discussed in Section 6.1.

After data collection and adequate training, the NN detector is implemented online and activated at the end of each material constraint period, with the process controlled by the modified LEMPC in Eq. 5 with combined open-loop and closed-loop control described in Section 5. Since the feed-forward NN model is a static model that receives inputs of fixed dimension, N_T (which is the length of the time-varying trajectory over one material constraint period N_p), the detection window of the NN detector when activated online is $N_T = N_p$. The detector will receive the entire sequence of full state measurements $\bar{x}(t_k)$ over the latest material constraint period with a fixed length N_T. Each sample consists of a two-dimensional matrix $n \times N_T$, where n is the full state dimension, and N_T is the length of each state trajectory within the detection window. Each training sample corresponds to a different set of initial conditions for the closed-loop system simulation, and equal number of samples within each class labels are collected to ensure training accuracy.

6.1. Choice of detection input variable

The nonlinear system of Eq. 1 is operated in an off steady-state manner under LEMPC by maximizing a nonlinear function of process state vector with respect to the control actions, which are subject to their respective lower and upper bounds, and material consumption constraints. Considering this, the exact trajectory of each individual state variable is not predictable and does not follow a general expected trend even under nominal operation. Therefore, assessing the trajectory of the measured state vector is not an effective method of detecting the occurrence of a cyber-attack.

Moreover, if the goal of a cyber-attack is to destabilize the closed-loop system within the shortest amount of time, the attacker will choose to set the current state measurement to the maximum/minimum allowable attack value characterized by the boundary of the secure operating region $\Omega_{\rho_{secure}}$ such that no alarms will be triggered. Therefore, the falsified sensor measurements will also yield a Lyapunov function that is equal to ρ_{secure}. Unlike the case of operation under tracking MPC where the Lyapunov function decreases as the process states are driven towards the origin, off steady-state operation of LEMPC results in a state trajectory that remains on the boundary of the secure operating region $\Omega_{\rho_{secure}}$ where $V(\bar{x}) = \rho_{secure}$ for the majority of each material constraint period as discussed in Section 3.1. Therefore, the trajectory of the Lyapunov function $V(\bar{x})$ under nominal operation and under cyber-attacks can be too similar to differentiate. For these reasons, the control Lyapunov function of the full-state measurements $V(\bar{x})$, which is used as an input variable for the detection algorithm used together with a tracking MPC (Chen et al., 2020), is no longer a good measure of input for the detection algorithm when the system is operated under LEMPC.

Given that EMPC optimizes the economic benefit in its cost function, the progression of economic benefit is a measure that effectively reflects the time-varying operation under LEMPC; hence,

information derived from the economic benefit provides a good comparison for attacked and not-attacked scenarios. Therefore, we will be monitoring the evolution of economic benefits during closed-loop operation. The cumulative economic benefit increases monotonically as operation time progresses. The first derivative of cumulative economic benefit (i.e., incremental economic benefit, which can be analogous to the reaction rate of desired product, at each sampling period) displays varying patterns depending on the initial conditions and on the material consumption constraint. The rate of change in the incremental economic benefit, or the change in the production reaction rate between sampling periods, provides information on the rate of change in the optimized cost function l_e inside the integral in Eq. 5a. This rate of change, which is also the second derivative of the cumulative economic benefit, will be used as the input parameters $p(\tilde{x})$ for the neural-network-based detection algorithm.

Remark 4. Material constraints on the feed stock are commonly seen in the industry. Moreover, operating the process in an off-steady-state manner with material constraint periods imposed is a common practice for economic model predictive control because we would like to compare its control performance to that of the process operated at steady-state for all times. While EMPC aims to maximize economic benefits by computing optimal sets of control actions, we impose this constraint on EMPC such that the sum of the calculated control actions will be the same as the sum used in steady-state operation. Depending on the initial conditions, the state trajectory may exhibit different patterns when the material constraint is removed. Despite this, the proposed neural-network detection approach does generalize to systems without material constraint periods. This is because the neural network detector, with adequate training, is still able to distinguish the attacked trajectory from the nominal trajectory of the examined detection variable (in our case, the second time-derivative of the economic objective function).

7. Application to a nonlinear chemical process

7.1. Process description and control system design

The application of the modified LEMPC of Eq. 5, the resilient control strategy presented in Section 5, as well as the training and online detection of NN cyber-attack detectors are demonstrated on a chemical process example. Specifically, the process considered is a well-mixed, non-isothermal continuous stirred tank reactor (CSTR), within which an irreversible second-order exothermic reaction takes place. The second-order reaction, $A \rightarrow B$, transforms reactant A to product B at a reaction rate $r_B = k_0 e^{-E/(RT)} C_A^2$. The CSTR is equipped with a heating jacket that supplies or removes heat at a rate Q. The dynamic model of this CSTR process is described by the following material and energy balance equations:

$$\frac{dC_A}{dt} = \frac{F}{V}(C_{A0} - C_A) - k_0 e^{\frac{-E}{RT}} C_A^2 \tag{13a}$$

$$\frac{dT}{dt} = \frac{F}{V}(T_0 - T) + \frac{-\Delta H}{\rho_L C_p} k_0 e^{\frac{-E}{RT}} C_A^2 + \frac{Q}{\rho_L C_p V} \tag{13b}$$

where C_A is the concentration of reactant A in the reactor, V is the volume of the reacting liquid in the reactor (assuming the vessel has constant holdup), T is the temperature of the reactor and Q denotes the heat input rate. The concentration of reactant A in the feed is C_{A0}. The feed temperature and volumetric flow rate are T_0 and F, respectively. The reacting liquid has a constant density of ρ_L and a heat capacity of C_p. ΔH, k_0, R, and E represent the enthalpy of reaction, pre-exponential constant, ideal gas constant, and activation energy, respectively. A complete list of the process parameter values are shown in Table 1.

The CSTR is initially operated at the unstable steady-state $[C_{As},\ T_s] = [1.9537\ kmol/m^3,\ 401.87\ K]$, and $[C_{A0_s}\ Q_s] = [4\ kmol/m^3,\ 0\ kJ/hr]$. The manipulated inputs are the inlet concentration of reactant A and the heat input rate, which are represented by the deviation variables $\Delta C_{A0} = C_{A0} - C_{A0_s}$, $\Delta Q = Q - Q_s$, respectively. The manipulated inputs are bounded as follows: $|\Delta C_{A0}| \leq 3.5\, kmol/m^3$ and $|\Delta Q| \leq 5 \times 10^5\, kJ/hr$. Therefore, the states and the inputs of the closed-loop system are $x^T = [C_A - C_{As}\ \ T - T_s]$ and $u^T = [\Delta C_{A0}\ \ \Delta Q]$, respectively, such that the equilibrium point of the system is at the origin of the state-space, (i.e., $x_s^T = [0, 0], u_s^T = [0, 0]$). We assume that at time $t = t_0$, the system is at the equilibrium point (i.e., the initial conditions of the system are $x_0 = [0, 0]^T$).

The control objective is to maximize the economic profit of the CSTR process of Eq. 13 by manipulating the inlet concentration ΔC_{A0} and the heat input rate ΔQ, while maintaining the closed-loop state trajectories in the stability region Ω_ρ for all times under LEMPC. The objective function of the LEMPC optimizes the production rate of B as follows:

$$l_e(\tilde{x}, u) = r_B(C_A, T) = k_0 e^{-E/RT} C_A^2 \tag{14}$$

The dynamic model of Eq. 13 is numerically simulated using the explicit Euler method with an integration time step of $h_c = 2.5 \times 10^{-5}\ hr$. The nonlinear optimization problem of the LEMPC of Eq. 5 is solved using the MATLAB OPTI Toolbox with the sampling period $\Delta = 2.5 \times 10^{-3}\ hr$.

The modified LEMPC of Eq. 5 uses the following material constraint to make the averaged reactant material available within one operating period $t_{N_p} = 0.06\ hr$ to be its steady-state value, C_{A0s} (i.e., the averaged reactant material in deviation form, u_1, is equal to 0).

$$\frac{1}{t_{N_p}} \int_0^{t_{N_p}} u_1(\tau) d\tau = 0\ kmol/m^3 \tag{15}$$

The control Lyapunov function $V(x) = x^T P x$ is designed with the following positive definite P matrix:

$$P = \begin{bmatrix} 1060 & 22 \\ 22 & 0.52 \end{bmatrix} \tag{16}$$

The closed-loop stability region Ω_ρ for the CSTR with $\rho = 320$ is characterized as a level set of Lyapunov function inside the region D, from which the origin can be rendered asymptotically stable under the controller $u = \phi(x) \in U$ of Eq. 3. The secure operating region $\Omega_{\rho_{secure}}$ for the LEMPC in Eq. 5 is selected to have $\rho_{secure} = 90$. The matrix P in $V = x^T P x$ and the stability region Ω_ρ are determined through simulations when determining the largest invariant set Ω_ρ in state-space (i.e., the level set of V) in which $\dot{V}$ is rendered negative ($\dot{V} \leq -\alpha_3(|x|)$, where α_3 is a class $\mathcal{K}$ function) for all states within Ω_ρ under the stabilizing controller $u = \phi(x) \in U$. Different values of P will generate different set of states where $\dot{V} \leq -\alpha_3(|x|)$, resulting in a different size and shape of the invariant set Ω_ρ.

Remark 5. The closed-loop system exhibits periodic patterns due to the periodic reactant material constraint imposed on the control actions. The process itself is not periodic; however, the material constraint imposed on the control actions renews periodically.

Table 1
Parameter values of the CSTR.

$T_0 = 300$ K	$F = 5$ m^3/h
$V = 1$ m^3	$E = 5 \times 10^4$ kJ/kmol
$k_0 = 8.46 \times 10^6$ m^3/kmol h	$\Delta H = -1.15 \times 10^4$ kJ/kmol
$C_p = .231$ kJ/kg K	$R = 8.314$ kJ/kmol K
$\rho_L = 1000$ kg/m^3	$C_{A0_s} = 4$ kmol/m^3
$Q_s = 0.0$ kJ/h	$C_{A_s} = 1.95$ kmol/m^3
$T_s = 401.87$ K	

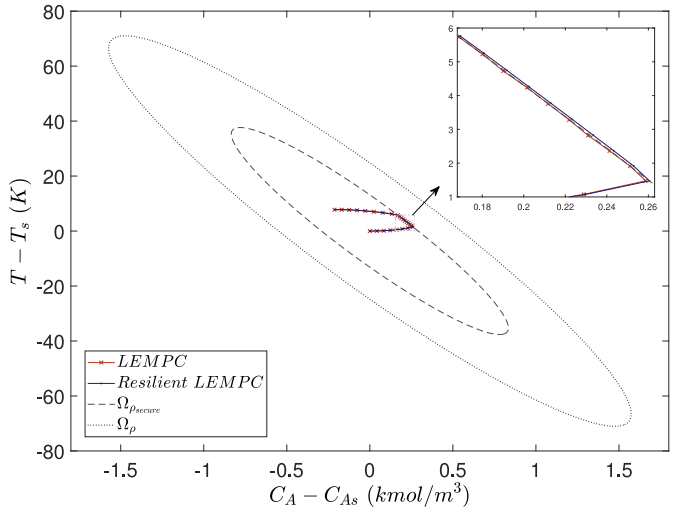


Fig. 4. State-space plot showing the evolution of measured process states over one material constraint period under LEMPC (red trajectory) and under resilient LEMPC (blue trajectory). (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

Remark 6. The design of the secure operating region $\Omega_{\rho_{secure}}$ can be adjusted depending on the system dynamics, the desired threshold for economic benefits, the magnitude and type of cyber-attacks, as well as whether the detector experiences time delay in correctly identifying the attacks. If the process dynamics are very fast, then more room needs to be vacated between Ω_ρ and $\Omega_{\rho_{secure}}$ to accommodate for the fast changes in process states when under cyber-attacks. However, designing a conservative secure operating region $\Omega_{\rho_{secure}}$ is at the expense of compromising economic benefits, since the maximum economic gain under normal operation is bounded by $\Omega_{\rho_{secure}}$. Therefore, the determination of the size of $\Omega_{\rho_{secure}}$ comes from a balance between operational stability and economic performance. These were all factors taken into consideration when running extensive closed-loop simulations to determine the value of ρ_{secure}.

7.2. Resilient operation of LEMPC

With initial conditions $x_0 = [0, 0]^T$, the closed-loop operation of the CSTR process in Eq. 13 over one material constraint period t_{N_p} under the modified LEMPC in Eq. 5, and under the resilient control of LEMPC with combined open-loop and closed-loop control actions as described in Section 5 around the secure operating region $\Omega_{\rho_{secure}}$ are both carried out. Fig. 4 presents the state-space plot showing the trajectory of the measured process states using the modified LEMPC of Eq. 5 and using the resilient LEMPC control strategy when the process is under no attack. The switching from using closed-loop to open-loop control actions happens at $t_s = 0.0175$ h. For $t_0 \leq t_k < t_s$, measured process states are well within the secure operating region $\Omega_{\rho_{secure}}$, and closed-loop control using the modified LEMPC of Eq. 5 is used with state feedback updates. The LEMPC of Eq. 5 is deactivated at $t_s = 0.0175$ h when the measured process states first reach the boundary of the secure operating region, and can no longer be trustworthy as this may be a result of a cyber-attack, i.e., when $\rho_{secure} - V(\bar{x}(t_k)) \leq c$, where $c = 0.5$ for this case study. The distance from the secure region boundary, c, is determined to account for computational error in designing and inserting the attacked sensor measurements. It provides a buffer zone for which resilient LEMPC can be activated accurately and preemptively. Therefore, for $t_s \leq t_k \leq t_{N_p}$, control actions $u'(t_k)$ from the open-loop optimization of Eq. 10 that are solved based on the initial condition x_0 will be applied.

Even in the case that no process disturbance, no model mismatch, and no cyber-attack is present, the resulting state trajectories under LEMPC (closed-loop only), and the resilient LEMPC (closed-loop followed by open-loop control actions after the switching time t_s) are slightly different. This is because the prediction horizon used in the ordinary LEMPC with periodic closed-loop feedback has a length of $N = 8$ and rolls forward in time as feedback signal updates are received, whereas the open-loop optimization problem computed at the beginning of the material constraint period accounts for $N_p = 24$. Therefore, the control actions computed from the open-loop optimization, $u'(t_k)$, will be slightly different from $u(t_k)$ calculated from online optimization, resulting in slightly different state trajectories.

Despite the subtle differences in the state trajectory, using open-loop control actions following closed-loop control still maintains the process states within the secure operating region (hence the stability region) for all times. It is important to note that, if the process is operated at steady-state, the total economic benefit in the form of $\int_{t_0}^{t_{N_p}} l_e(\bar{x}(t))dt$ is 0.6397 kmol/m^3, which is much less than that achieved under time-varying EMPC operation. The total economic benefit from t_0 to t_{N_p} using closed-loop-only control actions from the LEMPC of Eq. 5 is 0.8192 kmol/m^3, and using the resilient control strategy outlined in Section 5 is similarly 0.8203 kmol/m^3. Under no disturbances or model mismatch, the total economic benefit achieved by the resilient LEMPC using open-loop control actions is marginally higher. In closed-loop operation, we used a shorter prediction horizon to speed up the computation to ensure the real-time implementation of EMPC. Since the optimization problem of EMPC is essentially non-convex, the solutions we obtained from closed-loop operation may not be as good as the solutions calculated at the beginning, which uses a sufficiently long prediction horizon that covers the entire operating period as per material constraints. This shows the effectiveness of the resilient control strategy when the system is under no attack as it does not compromise system stability and economic performance. Furthermore, the similarity in the two trajectories also suggests that, if a cyber-attack is present and the resilient control strategy is utilized, the evolution of true process states will highly resemble that under closed-loop control in the absence of cyber-attacks. Under min-max attacks with LEMPC operation, the total economic benefit that the true process states provide is 1.4939 kmol/m^3; the higher economic benefit is a result of the min-max attacks driving the true states outside of the stability region. With resilient LEMPC operation and under min-max attacks, the true process states also yield a total economic benefit of 0.8203 kmol/m^3 over one operating period, which is the same as the case under no attacks. Since NN detection is activated at the end of the first operating period, the total economic benefit with integrated NN detection is also 0.8203 kmol/m^3. This demonstrates that when the process operates under resilience LEMPC, the addition of cyber-attacks does not alter the economic performance over one material constraint period.

7.3. Cyber-attack resiliency assessment

The purpose of using the resilient control strategy outlined in Section 5 is to prevent true process states from exiting the stability region Ω_ρ when under sensor cyber-attacks. Fig. 5 shows the state-space plot of the evolution of true process states and attacked state measurements from initial conditions $x_0 = [0, 0]^T$ over one material constraint period under LEMPC and under resilient LEMPC when the temperature sensor is attacked by min-max, geometric, replay and surge attacks, respectively. In all cases, once the specified cyber-attack starts, it will continue until it has been successfully detected; the detection results and process simulation

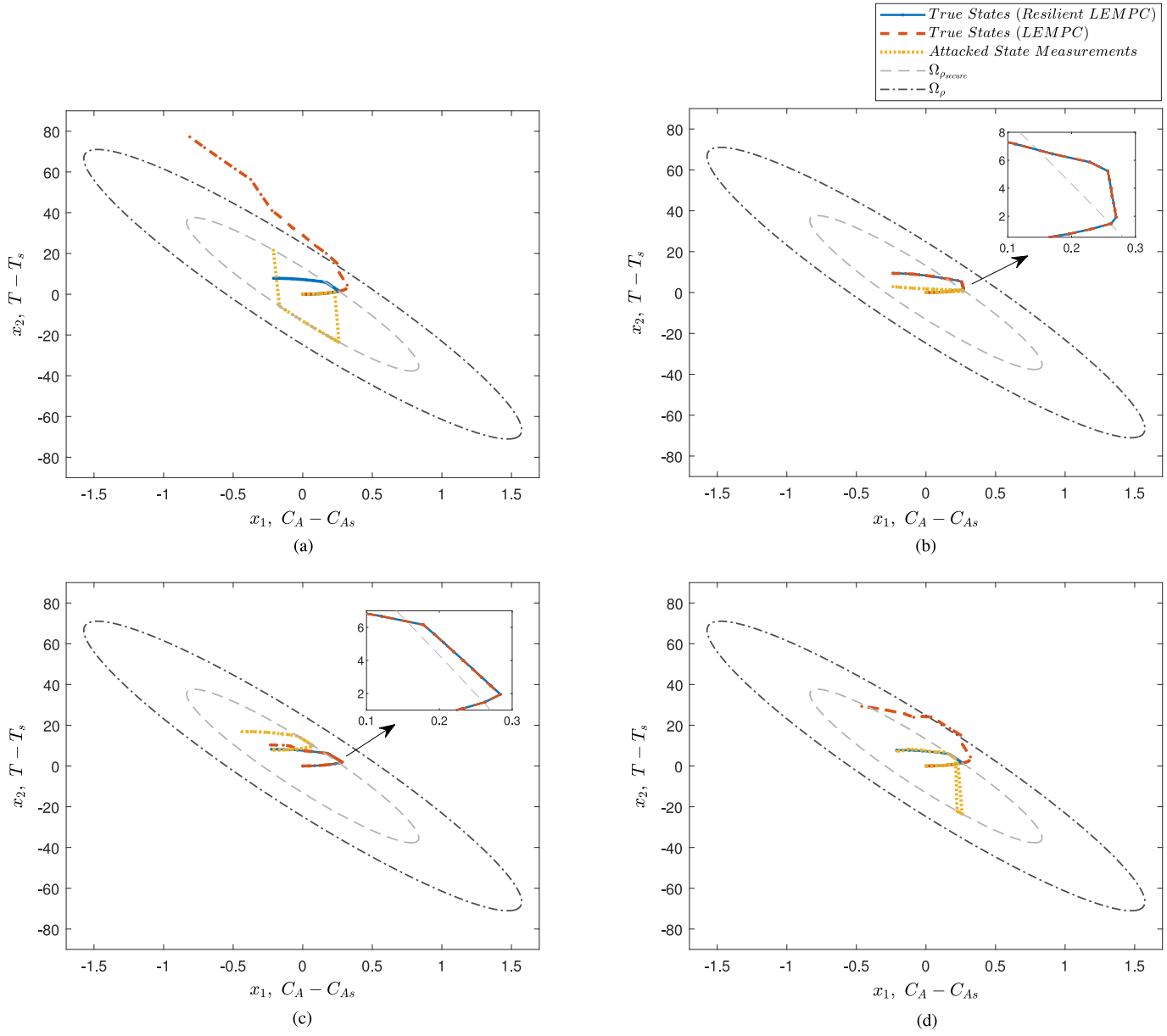


Fig. 5. State-space plot showing the evolution of true process states and attacked state measurements (yellow trajectories) over one material constraint period under LEMPC (red trajectories) and under resilient LEMPC (blue trajectories) when (a) min-max, (b) geometric, (c) replay, and (d) surge attacks, are targeting the temperature sensor, where the dash-dotted ellipse is the stability region Ω_ρ and the dashed ellipse is $\Omega_{\rho_{secure}}$. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

after the detection are shown in Section 7.5. Here, the simulation results over only one material constraint period are shown. After a cyber-attack has tampered the sensor, the resulting falsified state measurements will not exit the secure operating region $\Omega_{\rho_{secure}}$ so as to stay inconspicuous to the control engineer.

Min-max and surge cyber-attacks are added at $t = t_s = 0.0175$ h such that there will be no suspicious deviation in the Lyapunov function of the system. At $t = 0.0175$ h, both the true process state and the attacked state measurement will reach the boundary of the secure operating region, $V(x(t_s)) = V(\tilde{x}(t_s)) = \rho_{secure}$. As shown in Fig. 5(a) and (d), when the temperature sensor is under min-max and surge attacks respectively, true process states will exit $\Omega_{\rho_{secure}}$ and eventually Ω_ρ if only closed-loop control actions from the online LEMPC optimization in Eq. 5 are used. However, when the resilient LEMPC control strategy is implemented, closed-loop control is deactivated at $t = 0.0175$ h, and the falsified feedback measurements can no longer impact the control system. Open-loop control actions, which are calculated based on a correctly measured set of initial conditions, are used starting at $t = 0.0175$ hr until the end of the material constraint period when $t = t_{N_p} = 0.06$ h. As a result, the true process states will not exit $\Omega_{\rho_{secure}}$, and the evolution of the true process states is almost identical to that under secure closed-loop control (as demonstrated in Section 7.2). The system stays resilient to min-max and surge attacks, with protected stability and comparable control performance.

However, the resilient control strategy may not be effective when the system is under other types of attacks, particularly in situations where the falsified state measurement does not approach the boundary of $\Omega_{\rho_{secure}}$. To illustrate this, geometric attacks on the temperature measurements as shown in Fig. 5(b) start at $t = 0.01$ h following Eq. 8, where $\beta = x(t) * (1.001)$ and $\alpha = 0.1$. As cyber-attacks could happen at any time instant during operation, geo-

metric attacks are designed and inserted as such to demonstrate the incapability of the resilient control strategy in handling geometric attacks or attacks alike. At $t = 0.01$ h, the states have not reached the boundary of $\Omega_{\rho_{secure}}$, therefore not satisfying the condition for deactivating closed-loop control. Geometric attacks starting at $t = 0.01$ h resulted in state measurements that did not reach the boundary of $\Omega_{\rho_{secure}}$ for the entire duration of cyber-attack. Hence, closed-loop control continued with these false measurements, and the true process states exited $\Omega_{\rho_{secure}}$ during operation. Despite having a correct array of open-loop control actions computed at $t = 0$ h using the correctly measured initial conditions, these control actions were not used. As a result, the resilient control strategy fails to ensure that the true process states are maintained within the secure operating region $\Omega_{\rho_{secure}}$.

Moreover, there may be situations where, even when closed-loop control is deactivated and feedback measurements are no longer used, the true process states still exit $\Omega_{\rho_{secure}}$ because the open-loop control actions are calculated based on false sensor measurements. To illustrate this scenario, replay attacks as shown in Fig. 5(c) start at $t_0 = 0$ h, and the replayed signals span the duration of one material constraint period. In other words, the replayed signals are real closed-loop state measurements when the system started from a different set of initial conditions, $\bar{x}_0 = [-0.2107\ kmol/m^3; 7.8047\ K]$. Since the initial conditions $\bar{x}_0$ are incorrect, open-loop control actions optimized over the prediction horizon of N_p based on $\bar{x}_0$ are also not correct. As a result, despite the falsified state measurements also reaching the boundary of $\Omega_{\rho_{secure}}$ at $t = 0.0175$ h and deactivating closed-loop control, these incorrect open-loop control actions applied on the process still resulted in true process states exiting the secure operating region.

In this example, when under geometric and replay attacks, the true process states did not exit the stability region Ω_ρ; however, this may not be the case for a different geometric attack with larger α (geometric factor), a different replay attack that yielded more aggressive open-loop control actions, or for a faster process. In other words, system stability cannot be guaranteed by using the resilient control strategy, and an effective cyber-attack detection mechanism needs to be included.

7.4. Detectors training and testing

To train neural-network detectors, training data will be collected under closed-loop operation with the secure LEMPC outlined in Eq. 5. Simulation period is one material constraint period $t_{N_p} = 0.06\ hr$ with $N_p = 24$. Cyber-attacks are added at random times and last until the end of the simulation period. Neural network models are constructed and trained using the MATLAB Machine Learning and Deep Learning Toolboxes.

The reaction rate to yield product B, $r_B(\bar{x})$ can be calculated from full-state measurements $\bar{x}(t)$ at each time instant t_k from $k = 0$ to $k = N_p$ following Eq. 14, where $C_A = \bar{x}_1 + C_{A_s}$ and $T = \bar{x}_2 + T_s$. The input parameters used for neural network training are the time-varying trajectory of the rate of change in $r_B(\bar{x})$ over the simulation period of one material constraint period $N_p = 24$, which is denoted as $p(\bar{x})$, shown as follows:

$$p(\bar{x}(t)) = \frac{dr_B(\bar{x})}{dt} \tag{17}$$

The evolution of $p(\bar{x})$ when the temperature sensor is under no attack, and under min-max, geometric, replay, and surge attacks, are shown in Fig. 6. Each sample consists of a 1×24 array of $p(\bar{x})$, started from a different initial condition within Ω_ρ. With extensive closed-loop simulations, equal number of samples are collected for each output label, from which 70% are used for training, and 30% are used for testing.

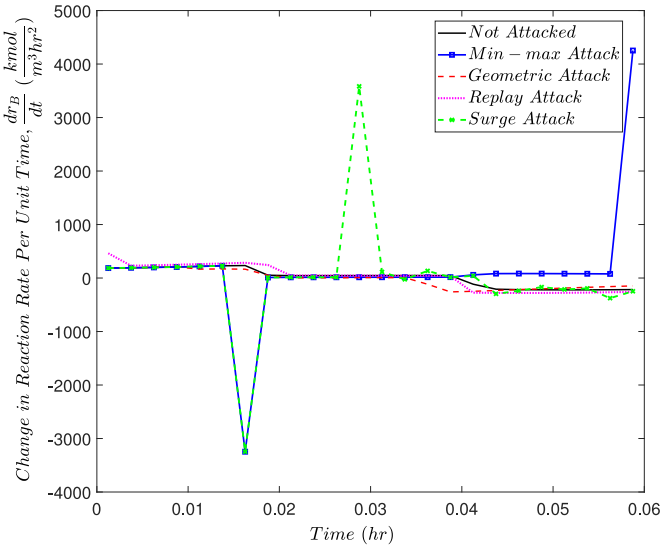


Fig. 6. Time-derivative of the reaction rate r_B of Eq. 14 based on measured process states over one material constraint period, when the temperature sensor is under no attack, and under min-max, geometric, replay, and surge attacks, respectively.

First, min-max attacks are used to train a neural-network-based detector. This feed-forward neural network model has two hidden layers with 12 and 10 neurons in each layer respectively. Both hidden layers use a *tansig* activation function, which is in the form $g_{1,2}(z) = \frac{2}{1+e^{-2z}} - 1$. The output layer uses a *softmax* function to provide a predicted probability of the class labels, which is in the form of $g_3(z_j) = \frac{e^{z_j}}{\sum_{i=1}^{H} e^{z_i}}$ where H denotes the number of class labels. Bayesian regularized mean squared error cost function $S(w)$ are minimized with respect to the weights and biases using the Levenberg–Marquardt algorithm, in which the gradient and the Hessian matrix of $S(w)$ are calculated using the back-propagation method. A total of 750 samples are collected for each class label. The training time for this 2-class detector is 2.05 s, undergoing 70 epochs, and the detector achieves a training accuracy of 98.9%. The testing accuracy of this detector against the different attack types is shown in Table 2. Note that geometric attacks are not identified as being attacked due to the vast difference in the trends of $p(\bar{x})$ when under geometric attack compared to min-max attacks as shown in Fig. 6.

A second detector is trained with min-max and geometric attacks. The detector is able to classify between 3 classes: Not attacked, attacked by min-max cyber-attacks, and attacked by geometric cyber-attacks. Thus, the detector is capable of differentiating the types of cyber-attacks in addition to indicating the presence of one. This detector is trained because geometric attacks exhibit very different behavior than min-max attacks, and therefore the testing accuracy by the 2-class detector is very low. This 3-class feed-forward neural network detector has two hidden layers with 15 and 12 neurons each, using the same activation functions and cost function in Eq. 11, which is minimized using the Levenberg–Marquardt algorithm. The training time for this 3-class detector is 39.48 s with 300 epochs. This 3-class detector achieves an overall training accuracy of 91.8%, and its testing accuracies in response to min-max, geometric, and surge attacks are shown in Table 2. The detector accurately identifies min-max and geometric attacks as their respective labels, and it classifies 71.0% of surge attacks as min-max, 10.0% as geometric, and the remaining 19.0% are wrongly classified as “not attacked”.

Remark 7. Since replay signals could mimic the secure operation of one entire material constraint period starting at a different ini-

Table 2
Detection accuracies of NN detectors in response to min-max, geometric, and surge attacks.

	Detector 1 (Attacked vs. Not Attacked)	Detector 2 (Min-max vs. Geometric vs. Not Attacked)
Min-max	98.3%	89.7%
Geometric	2.4% (Attacked)	71.1%
Surge	87.0% (Attacked)	71.0% (Min-max); 10.0% (Geometric)
Not Attacked	98.4%	95.6%

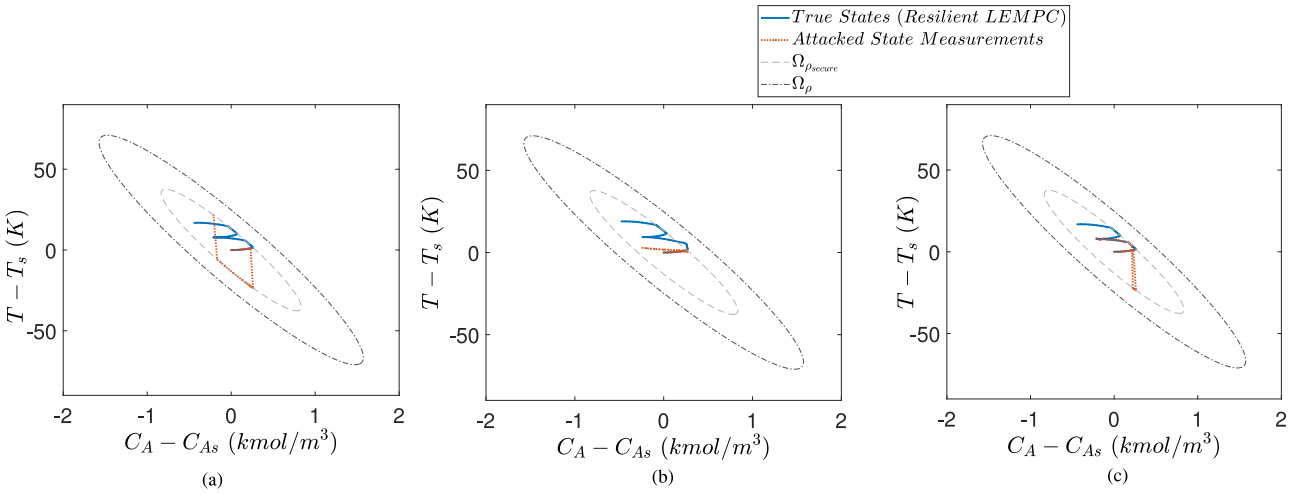


Fig. 7. State-space plot showing the evolution of true process states (blue trajectories) and attacked state measurements (red trajectories) over two material constraint periods under the resilient LEMPC when (a) min-max, (b) geometric, and (c) surge attacks, targeting the temperature sensor are successfully detected by a NN detector at the end of the first material constraint period, $t = 0.06$ *hr*, where the dash-dotted ellipse is the stability region Ω_ρ and the dashed ellipse is $\Omega_{\rho_{secure}}$. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

tial condition, they are essentially a different sample that belongs to the class of "not attacked", and will be rightfully classified as being "not attacked". At the end of the material constraint period, the falsified signals follow exactly the trajectory of previous secure measurements of one period, thus they will remain undetectable by the NN detectors. Since the NN approach used in this study is based on supervised classification, it is heavily dependent on labeled data from distinct classes. Being duplicates of nominal signals, replay signals are not in a distinct class of signals that is different from the nominal data, thus the proposed NN approach is an unsuitable detection method for replay attacks. Purely data-based approaches examining sensor measurements in the case of replay attacks will not be sufficient, and model-based prediction approaches may be a possible future research direction. The reader may refer to other works on the detection of replay attacks in Hoehn and Zhang (2016); Tran et al. (2013).

7.5. Online detection

Detector 1 is used to detect min-max and surge attacks, whereas detector 2 is used to detect geometric attacks. The corresponding detector is activated at the end of the material constraint period, and examines state measurements received over the last material constraint period. Since replay attacks cannot be detected, the online detection results are also not shown.

Fig. 7 shows the evolution of true process states and measured process states attacked by min-max, geometric, and surge cyber-attacks when the process is controlled by the resilient LEMPC with combined open-loop and closed-loop control. The figures show the trajectories over two material constraint periods, where NN-based detection occurs twice – once at the end of the first period, and once at the end of the second period.

Min-max and surge attacks are correctly detected by detector 1 at the end of the first constraint period $t = 0.06$ h by examining the trajectory of $p(\bar{x}(t))$ from $t = 0$ h to $t = 0.06$ h, after which the sensor devices are switched to a secure set of redundant sensors and operation continues with these secure sensor measurements. During the second period, the attacked old set of sensors are no longer connected to the control system, and the newly switched set of sensors are not tampered by cyber-attacks. At the end of the second material constraint period $t = 0.12$ h, detector 1 is activated again, and it correctly classifies the secure measurements as "not attacked".

Furthermore, if a particular attack type is trained as a separate class (i.e., "geometric") from other attack types (i.e., "min-max"), then the detector is also capable of identifying the type of cyber-attack. As shown in Fig. 7(b), although the true process states exited $\Omega_{\rho_{secure}}$ during the first material constraint period (closed-loop control based on false feedback signals was not deactivated), the state measurements attacked by geometric attacks were still correctly identified as geometric by detector 2 at the end of the first material constraint period. After switching the sensor devices to the respective secure back-up sensors, detector 2 correctly identifies the trajectory of $p(\bar{x}(t))$ over the second material constraint period from $t = 0.06$ h to $t = 0.12$ h as "not attacked". This means that, although the resilient control strategy cannot ensure stability over one material constraint period if the attacked measurement deliberately avoids approaching the boundary of $\Omega_{\rho_{secure}}$, the attack can still be detected at the end of the material constraint period, and mitigation measures can be taken following the successful detection to terminate the impact of the cyber-attacks. One method to avoid the true states from exiting the stability region when under geometric attacks is to adjust the size of $\Omega_{\rho_{secure}}$ such that the resilient control strategy could come into effect earlier. Moreover, setting a shorter material constraint period in addition to operating within a conservative secure region could be another preventative method to consider, so that the cyber-attack detection can happen more frequently.

8. Conclusion

In this work, the secure operation of nonlinear chemical processes under economic model predictive control was presented via the design of a secure operating region, resilient control strategies, and a neural-network-based cyber-attack detector. Considering a general class of nonlinear systems, a resilient Lyapunov-based Economic Model Predictive Controller with combined closed-loop and open-loop control action implementation was developed at the cost of reduced total economic gain. Through simulating a continuously stirred tank reactor process, it was demonstrated that the proposed control strategy was effective in maintaining process stability against particular types of malicious cyber-attacks, namely min-max and surge attacks, while achieving comparable economic performance compared to nominal operation under no attacks. Two neural-network-based cyber-attack detectors were constructed to detect the presence or distinguish the type of a cyber-attack, and the time-varying trajectory of a nonlinear function of sensor measurements were used as the input variables for the detection algorithm. The detector was able to provide a diagnosis at the end of each LEMPC operation period, and simulation results demonstrated that min-max, surge, and geometric attacks could be successfully detected.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Scarlett Chen: Conceptualization, Methodology, Software, Writing - original draft. **Zhe Wu:** Conceptualization, Methodology, Software, Writing - original draft. **Panagiotis D. Christofides:** Supervision, Writing - review & editing.

References

Agrawal, S., Agrawal, J., 2015. Survey on anomaly detection using data mining techniques. Procedia Comput. Sci. 60, 708–713.

Ahlén, A., Akerberg, J., Eriksson, M., Isaksson, A., Iwaki, T., Johansson, K., Knorn, S., Lindh, T., Sandberg, H., 2019. Toward wireless control in industrial process automation: a case study at a paper mill. IEEE Control Syst. Mag. 39, 36–57.

Amin, S., Litrico, X., Sastry, S., Bayen, A., 2012. Cyber security of water scada systems part i: analysis and experimentation of stealthy deception attacks. IEEE Trans. Control Syst. Technol. 21, 1963–1970.

Amrit, R., Rawlings, J.B., Angeli, D., 2011. Economic optimization using model predictive control with a terminal cost. Annu. Rev. Control 35, 178–186.

Asghar, M., Hu, Q., Zeadally, S., 2019. Cybersecurity in industrial control systems: issues, technologies, and challenges. Comput. Netw. 165, 106946.

Ashibani, Y., Mahmoud, Q., 2017. Cyber physical systems security: analysis, challenges and solutions. Comput. Secur. 68, 81–97.

Bishop, C., 2006. Pattern recognition and machine learning (information science and statistics). Springer-Verlag New York, Inc..

Burden, F., Winkler, D., 2008. Bayesian Regularization of Neural Networks. In: Artificial Neural Networks. Springer, pp. 23–42.

Cárdenas, A., Amin, S., Lin, Z., Huang, Y., Huang, C., Sastry, S., 2011. Attacks against process control systems: risk assessment, detection, and response. In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, pp. 355–366.

Carter, B., Adams, S., Bakirtzis, G., Sherburne, T., Beling, P., Horowitz, B., Fleming, C., 2019. A preliminary design-phase security methodology for cyber–physical systems. Systems 7, 21.

Chaffart, D., Ricardez-Sandoval, L.A., 2018. Optimization and control of a thin film growth process: a hybrid first principles/artificial neural network based multiscale modelling approach. Comput. Chem. Eng. 119, 465–479.

Chamanbaz, M., Dabbene, F., Bouffanais, R., 2019. A Physics-based Attack Detection Technique in Cyber-physical Systems: A Model Predictive Control Co-design Approach. In: Proceedings of the 2019 Australian & New Zealand Control Conference (ANZCC). Auckland, New Zealand, pp. 18–23.

Chen, S., Wu, Z., Christofides, P.D., 2020. A cyber-secure control-detector architecture for nonlinear processes. AIChE J. 66, e16907.

Christofides, P.D., Davis, J., El-Farra, N., Clark, D., Harris, K., Gipson, J., 2007. Smart plant operations: vision, progress and challenges. AIChE J. 53, 2734–2741.

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

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

Falugi, P., Mayne, D.Q., 2013. Getting robustness against unstructured uncertainty: a tube-based mpc approach. IEEE Trans. Automat. Control 59 (5), 1290–1295.

Gavin, H., 2019. The Levenberg–Marquardt algorithm for nonlinear least squares curve-fitting problems.

Genge, B., Kiss, I., Haller, P., 2015. A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. Int. J. Crit. Infrastruct. Prot. 10, 3–17.

Gurney, K., 2014. An Introduction to Neural Networks. CRC press, London.

Hassan, C., Khan, M., Shah, M., 2018. Comparison of Machine Learning Algorithms in Data Classification. In: Proceedings of the 24th International Conference on Automation and Computing (ICAC). Newcastle upon Tyne, United Kingdom, pp. 1–6.

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

Hochreiter, S., Schmidhuber, J., 1997. Long short-term memory. Neural Comput. 9, 1735–1780.

Hoehn, A., Zhang, P., 2016. Detection of Replay Attacks in Cyber-physical Systems. In: Proceedings of the 2016 American Control Conference (ACC). Boston, MA, pp. 290–295.

Huang, L., Nguyen, X., Garofalakis, M., Hellerstein, J., Jordan, M., Joseph, A., Taft, N., 2007. Communication-efficient Online Detection of Network-wide Anomalies. In: Proceedings of the 2007 IEEE INFOCOM, 7. Anchorage, Alaska, pp. 134–142.

Humayed, A., Lin, J., Li, F., Luo, B., 2017. Cyber-physical systems security a survey. IEEE Internet Things J. 4, 1802–1831.

Kimaev, G., Ricardez-Sandoval, L.A., 2019. Nonlinear model predictive control of a multiscale thin film deposition process using artificial neural networks. Chem. Eng. Sci. 207, 1230–1245.

Lee, P., Clark, A., Bushnell, L., Poovendran, R., 2014. A passivity framework for modeling and mitigating wormhole attacks on networked control systems. IEEE Trans. Automat. Control 59 (12), 3224–3237.

Lin, Y., Sontag, E., 1991. A universal formula for stabilization with bounded controls. Syst. Control Lett. 16, 393–397.

Mayne, D., Kerrigan, E., Van Wyk, E., Falugi, P., 2011. Tube-based robust nonlinear model predictive control. Int. J. Robust Nonlinear Control 21 (11), 1341–1353.

Mohanty, S., Pradhan, A., Routray, A., 2007. A cumulative sum-based fault detector for power system relaying application. IEEE Trans. Power Deliv. 23, 79–86.

Omar, S., Ngadi, A., Jebur, H., 2013. Machine learning techniques for anomaly detection: an overview. Int. J. Comput. Appl. 79, 33–41.

Polycarpou, M., Ioannou, P., 1991. Identification and control of nonlinear systems using neural network models: Design and stability analysis. University of Southern California.

Raiyn, J., 2014. A survey of cyber attack detection strategies. Int. J. Secur.Appl. 8, 247–256.

Rawlings, J., Maravelias, C., 2019. Bringing new technologies and approaches to the operation and control of chemical process systems. AIChE J. 65, e16615.

Samanta, B., Al-Balushi, K., 2003. Artificial neural network based fault diagnostics of rolling element bearings using time-domain features. Mech. Syst. Signal Process. 17, 317–328.

Schuster, M., Paliwal, K., 1997. Bidirectional recurrent neural networks. IEEE Trans. Signal Process. 45, 2673–2681.

Sibi, P., Jones, S., Siddarth, P., 2013. Analysis of different activation functions using back propagation neural networks. J. Theoret. Appl. Inf. Technol. 47, 1264–1268.

Singh, J., Nene, M., 2013. A survey on machine learning techniques for intrusion detection systems. Int. J. Adv. Res.Comput. Commun. Eng. 2, 4349–4355.

Sun, Y., Yang, G., 2019. Robust event-triggered model predictive control for cyber–physical systems under denial-of-service attacks. Int. J. Robust Nonlinear Control 29, 4797–4811.

Tran, T., Shin, O., Lee, J., 2013. Detection of Replay Attacks in Smart Grid Systems. Proceedings of the 2013 International Conference on Computing, Management and Telecommunications. Ho Chi Min, Vietnam, pp. 298–302.

Tu, J., 1996. Advantages and disadvantages of using artificial neural networks versus logistic regression for predicting medical outcomes. J. Clin. Epidemiol. 49, 1225–1231.

Venkatasubramanian, V., 2019. The promise of artificial intelligence in chemical engineering: is it here, finally? AIChE J. 65, 466–478.

Widodo, A., Yang, B., 2007. Support vector machine in machine condition monitoring and fault diagnosis. Mech. Syst. Signal Process. 21, 2560–2574.

Wu, Z., Albalawi, F., Zhang, J., Zhang, Z., Durand, H., Christofides, P.D., 2018. Detecting and handling cyber-attacks in model predictive control of chemical processes. Mathematics 6, 173.

Wu, Z., Tran, A., Rincon, D., Christofides, P.D., 2019. Machine learning-based predictive control of nonlinear processes. part i: theory. AIChE J. 65, e16729.

Zhao, J., Wang, J., Yin, L., 2016. Detection and Control against Replay Attacks in Smart Grid. In: Proceedings of the 12th International Conference on Computational Intelligence and Security (CIS). Wuxi, China, pp. 624–627.