Chemical Engineering Research and Design 200 (2023) 312–324

Contents lists available at ScienceDirect

Chemical Engineering Research and Design

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

Encrypted decentralized model predictive control of nonlinear processes with delays

Yash A. Kadakia [a], Aisha Alnajdi [b], Fahim Abdullah [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

Keywords:
Model predictive control
Encrypted control
Nonlinear time-delay systems
Decentralized control
Cybersecurity
Process control

ABSTRACT

This work focuses on enhancing the operational safety, cybersecurity, computational efficiency, and closed-loop performance of large-scale nonlinear time-delay systems. This is achieved by employing a decentralized model predictive controller (MPC) with encrypted networked communication. Within this decentralized setup, the nonlinear process is partitioned into multiple subsystems, each controlled by a distinct Lyapunov-based MPC. These controllers take into account the interactions between subsystems by utilizing full state feedback, while computing the control inputs only corresponding to their respective subsystem. To address the performance degradation associated with input delays, we integrate a predictor with each LMPC to compute the states after the input delay period. The LMPC model is initialized with these predicted states. To cope with state delays, the LMPC model is formulated using differential difference equations (DDEs) that describe the state-delays in the system. Further, to enhance cybersecurity, all signals transmitted to and received from each subsystem are encrypted. A stability analysis is carried out for the encrypted decentralized MPC when it is utilized in a time-delay system. Bounds are set up for the errors arising from encryption, state-delays, and sample-and-hold implementation of the controller. Guidelines are established to implement this proposed control structure in any nonlinear time-delay system. The simulation results, conducted on a nonlinear chemical process network, illustrate the effective closed-loop performance of the decentralized MPCs alongside the predictor with encrypted communication when dealing with input and state delays in a large-scale process.

1. Introduction

Numerous large-scale industrial systems, such as power distribution grids, mechanical systems, chemical processes, and urban traffic networks, present a significant challenge as the system to be controlled is too large, resulting in a complex control problem to be solved. This challenge cannot be simply solved by using faster computers with larger memory. In response, decentralized control strategies have been proposed to address high dimensionality, constraints related to information structure, and inherent system delays in such systems (Bakule, 2008). In a decentralized setup, the overall system is divided into independent sub-systems that may be coupled with each other, but controlled by separate controllers, which together constitute a decentralized control structure. This provides a practical solution for reducing the computational complexity of a centralized control problem for a large-scale process.

Alongside dealing with large-scale processes, it is crucial to address the various sources of time delays that can impact control systems. These sources include the computation of control inputs for large-scale systems, communication lags during signal transfer, the inherent dynamics of material transportation within the process system, and control actuator dynamics. Using a decentralized control structure reduces a large, complex control problem into smaller sub-problems which are solved independently and simultaneously in different computing units. This reduces the delays due to control input computation. Advances in networked communication have simplified the interlinking, connectivity, and data transfer in cyber-physical systems and has made time-delays from communication negligible. However, delays due to control actuator dynamics in process networks cannot be compensated by smaller control input computation times or rapid transport of material in processes or rapid networked communication and, hence, need appropriate control strategies such as integrating a predictor within the controller design (Smith, 1957). Similarly, state delays in process networks cannot be completely eliminated by optimizing process layouts, and, hence,

[*] Corresponding author at: Department of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA 90095–1592, USA.
E-mail address: pdc@seas.ucla.edu (P.D. Christofides).

https://doi.org/10.1016/j.cherd.2023.10.041
Received 5 October 2023; Received in revised form 17 October 2023; Accepted 18 October 2023
Available online 21 October 2023

need to be accounted in the controller design.

Networked communication might make data transfer seamless and rapid. However, they are prone to cyberthreats. A breach or compromise within these systems could result in severe consequences, such as the disruption of critical services, physical harm, financial loss, and are also a threat to public safety. Recent developments in cyberattack techniques underscore the need to establish robust cybersecurity (Gandhi et al., 2011). Addressing cybersecurity concerns within industrial control systems primarily falls under the domain of operational technology (OT). Significant progress has been made in enhancing cybersecurity in the information technology (IT) sector, which focuses on the software aspects of systems, encompassing areas such as network architecture and data management. However, the field of cybersecurity within OT is currently trailing behind (Conklin, 2016). Various real-world examples underscore the importance of cybersecurity in networked cyber-physical systems and SCADA (Supervisory Control and Data Acquisition) environments. For instance, the cyberattack on SCADA controls responsible for managing the power grid in Ukraine in 2015 led to widespread power outages (Khan et al., 2016). Similarly, in the DarkSide ransomware attack on Colonial Pipeline in 2021, hackers encrypted its networked communication and demanded a ransom for the decryption keys. Consequently, Colonial Pipeline had to halt operations, causing disruptions in fuel distribution and financial losses (Tsvetanov and Slaria, 2021).

Extensive research has been conducted in areas such as developing machine learning-based cyberattack detectors (Al-Abassi et al., 2020; Dutta et al., 2020), using reachable set-based detection schemes (Narasimhan et al., 2023), employing linear encrypted controllers (Darup et al., 2018; Darup, 2020), analyzing the safety of process equipment when the system is under a cyberattack (Nieman et al., 2023), control switching techniques for attack detection (Narasimhan et al., 2022), process state recovery post cyberattack (Wu et al., 2020), and creating cyberattack-resilient controllers (Paridari et al., 2017). However, to the best of our knowledge, the development of cybersecure decentralized controllers for large-scale nonlinear processes with input and state delays remains an unexplored area, prompting our proposal for a novel control structure to address this challenge.

Specifically, we propose a decentralized control structure consisting of a set of Lyapunov-based MPCs, integrated with a predictor, utilizing encrypted networked communication. MPC is an advanced control strategy that achieves superior performance compared to traditional controllers via constraints, and optimizes critical performance metrics in multi-input multi-output systems. These advantages are derived from the utilization of a nonlinear mathematical model to predict future system behavior, and optimizing control inputs by minimizing a cost function with constraints. For large-scale systems, the control problem to be solved by a centralized MPC would be too complex. In contrast, a decentralized MPC divides this intricate problem into smaller, independent segments, concurrently solved in different edge computing units. In this configuration, we assume the presence of secure edge computers responsible for computing control inputs. Integrating a predictor within this setup serves to offset performance degradation due to input delays. To mitigate the influence of state-delays resulting from material transportation in systems, the process model employed by the LMPCs in the decentralized framework is based on differential difference equations. These equations account for the inherent state-delays present in the system. Further, the incorporation of encryption within the networked communication channels enhances cybersecurity as each edge computing unit receives and transmits encrypted signals.

The remainder of the paper is organized as follows: Section 2 presents preliminaries on notation, the general class of nonlinear systems considered, the system stabilizability assumptions, the cryptosystem used for employing encryption, and the effect of quantization. The encrypted decentralized MPC design, formulation of the MPCs, and stability analysis of the control scheme are presented in Section 3. In Section 4, closed-loop simulations of a nonlinear chemical process network with input and state delays under the encrypted decentralized LMPC system with and without predictor feedback are presented and discussed.

2. Preliminaries

2.1. Notation

The symbol $\|\cdot\|$ represents the Euclidean norm of a vector. $x^\top$ denotes the transpose of a vector x. $\mathbb{R}$, $\mathbb{Z}$, and $\mathbb{N}$ represent the sets of real numbers, integers, and natural numbers, respectively. $\mathbb{Z}_M$ denotes the additive groups of integers modulo M. Set subtraction is indicated by the symbol "$\backslash$", where $A\backslash B$ represents the set of elements that are in set A but not in set B. A function, $f(\cdot)$, falls under the class $\mathscr{C}^1$ if it is continuously differentiable within its defined domain. The term lcm(i, j) denotes the least common multiple of the integers i and j, while gcd(i, j) signifies the greatest common divisor, that divides i and j without any remainder.

2.2. Class of systems

This research focuses on multi-input multi-output (MIMO) nonlinear time-delay systems, characterized by a set of differential difference equations (DDEs), alternatively known as delay differential equations. These equations are formulated in the following manner:

$$\dot{x} = F(x, u) = f(x(t), x(t-d_1), u(t-d_2)) \tag{1}$$

The state vector is denoted by $x \in \mathbb{R}^n$, while $u \in \mathbb{R}^m$ represents the control input vector bounded by the set, $U \subset \mathbb{R}^m$. $d_1 > 0$ and $d_2 > 0$ are the state and input delays, respectively. The vector $f(\cdot)$ is a locally Lipschitz vector function of its arguments with $f(0, 0, 0) = 0$, rendering the origin as a steady state of Eq. (1). Without loss of generality, we assume the initial time as zero ($t_0 = 0$). Additionally, we define the set $S(\Delta)$ as the set of piece-wise constant functions characterized by a period of Δ. We consider $j = 1, \ldots, N_{sys}$ sub-systems, with each subsystem j consisting of states x_j which are regulated only by inputs u_j but potentially impacted by states in other subsystems due to coupling between subsystems. The continuous-time nonlinear dynamics of subsystem j is described as follows:

$$\dot{x}_j = F_j(x, u_j), \quad x_j(t_0) = x_{j_0}, \quad \forall j = 1, \ldots, N_{sys} \tag{2}$$

where N_{sys} denotes the number of subsystems, $x_j \in \mathbb{R}^{n_j}$ and $u_j \in \mathbb{R}^{m_j}$ are the state vector and control inputs for subsystem j, respectively. $x = [x_1^\top \ldots x_{N_{sys}}^\top]^\top \in \mathbb{R}^n$ is the state vector for the entire system, with $n = \sum_{j=1}^{N_{sys}} n_j$. $u = [u_1^\top \ldots u_{N_{sys}}^\top]^\top \in \mathbb{R}^m$ is the control input vector for the entire system, with $m = \sum_{j=1}^{N_{sys}} m_j$. The control input vector constraints are $u_j \in U_j := \{u_{min,j_i} \leq u_{j_i} \leq u_{max,j_i} \forall i = 1, \ldots, m_j\}$, $\forall j=1,\ldots,N_{sys}$. Hence, the set U that constrains the control input vector for the entire system is formed by the union of sets U_j, where $j = 1, \ldots, N_{sys}$. The system of Eq. (1) can be expressed as a perturbed form of the system without delays in the following manner:

$$\dot{x} = F(x, u, \xi) = f(x(t), x(t) + \xi_1(t), u(t) + \xi_2(t)) \tag{3a}$$

$$\xi_1 = x(t-d_1) - x(t) \tag{3b}$$

$$\xi_2 = u(t-d_2) - u(t) \tag{3c}$$

where $\xi^\top := [\xi_1^\top, \xi_2^\top] \in D \times U \in \mathbb{R}^{n+m}$ is the bounded perturbation vector for the state and input delays, and D is the open neighborhood around the origin.

Remark 1. In this research, we employ differential difference equations to characterize nonlinear time-delay systems. Differential difference equations (DDEs) fundamentally differ from ordinary differential equations (ODEs). One key distinction is that a dynamic system with an arbitrarily small delay is considered an infinite-dimensional system, even though the state vector would have finite dimension. Existing literature offers various approaches to describe nonlinear time-delay systems, such as first-order plus dead time and second-order plus dead time models. However, these methods are specific and assume certain linear model structures. Hence, we have opted to utilize nonlinear differential difference equations with constant delays in this study to ensure a more comprehensive analysis. Nevertheless, it is worth noting that other studies have utilized functional differential equations to describe nonlinear time-delay systems (Hale and Lunel, 1993), and our findings can potentially be extended to encompass such model structures as well.

2.3. Stability assumptions

Based on how the overall large-scale system is partitioned, there may exist interacting dynamics between the subsystems, as the states of one subsystem may impact the states of other subsystems. Accounting for these interactions, we assume the existence of stabilizing control laws $u_j = \Phi_j(x) \in U_j$, which regulate the individual subsystems $j = 1, \ldots, N_{sys}$, such that the origin of the overall system of Eq. (1) with $d_1 \equiv 0$ and $d_2 \equiv 0$ is rendered exponentially stable. This signifies the presence of a $\mathscr{C}^1$ control Lyapunov function $V(x)$ for which the following inequalities hold for all $x \in \mathbb{R}^n$ within an open region D surrounding the origin:

$$c_1|x|^2 \leq V(x) \leq c_2|x|^2, \tag{4a}$$

$$\frac{\partial V(x)}{\partial x} f(x, x, \Phi(x)) \leq -c_3|x|^2, \tag{4b}$$

$$\left|\frac{\partial V(x)}{\partial x}\right| \leq c_4|x| \tag{4c}$$

where c_1, c_2, c_3 and c_4 are positive constants, and $\Phi(x) = [\Phi_1(x)^\top \ldots \Phi_{N_{sys}}(x)^\top]^\top$ is the vector concatenating the stabilizing feedback control laws for all N_{sys} subsystems. For the nonlinear system described by Eq. (1), the region of closed-loop stability can be defined as a level set, Ω_ρ, of the control Lyapunov function V, such that $\Omega_\rho := \{x \in D | V(x) \leq \rho\}$, where $\rho > 0$. Hence, originating from any initial condition within Ω_ρ, the control input, $\Phi(x)$, guarantees that the state trajectory of the closed-loop system remains within Ω_ρ.

2.4. Paillier cryptosystem

In this research, we employ the Paillier cryptosystem (Paillier, 1999) to encrypt signals, specifically state measurements (x) and control inputs (u), transmitted to and from the controllers. Although we do not make use of the semi-homomorphic property of additive homomorphism within the Paillier cryptosystem, we employ it so that traditional controllers, such as proportional-integral controllers, which conduct computations in an encrypted space, can be integrated into the overall control architecture if required. The encryption procedure is initiated by generating the public and private key. The public key is used to encrypt integer messages into ciphertexts, and the private key is employed to decrypt ciphertexts and retrieve the original integer messages. The process of generating the public and private key can be outlined as follows:

1. Choose two large prime integers (p and q) randomly, ensuring, gcd (pq, $(p-1)(q-1)$) $= 1$.
2. Compute, $M = pq$.
3. Choose an arbitrary integer $\bar{g}$ such that $\bar{g} \in \mathbb{Z}_{M^2}$,which is the multiplicative group of integers modulo M^2.
4. Compute $\lambda = \text{lcm}(q-1, p-1)$.
5. Specify $\bar{L}(x) = (x-1)/M$.
6. Verify the existence of the subsequent modular multiplicative inverse: $u = (\bar{L}(\bar{g}^\lambda \bmod M^2))^{-1} \bmod M$.
7. If the inverse does not exist, revisit step 3 and select an alternate value of $\bar{g}$. If the inverse exists, $(M, \bar{g})$ is the public key and (λ, u) is the private key.Once the keys are acquired, the public and private keys are distributed to authorized recipients for encryption and decryption, respectively. The encryption process is as follows:

$$E_M(m, r) = c = \bar{g}^m r^M \bmod M^2 \tag{5}$$

where r is a randomly selected integer from the set $\mathbb{Z}_M$, and c represents the ciphertext achieved through the encryption of m. The decryption procedure is as follows:

$$D_M(c) = m = \bar{L}(c^\lambda \bmod M^2)u \bmod M \tag{6}$$

The aforementioned procedure can be demonstrated in a numerical example as follows:

Key generation steps:

1. Select 2 prime numbers $p = 13$, and $q = 17$.
2. $M = p \times q = 13 \times 17 = 221$.
3. Chose, $\bar{g} = 8$ which can be any integer between 1 and M^2.
4. Calculate $\lambda = \text{lcm}(q-1, p-1) = \text{lcm}(16, 12) = 48$.
5. Verify the existence of $u = 172$.
6. The public key is $(M, \bar{g}) = (221, 8)$.
7. The private key is $(\lambda, u) = (48, 172)$.

Encryption:

1. The message to be encrypted is $m = 3$.
2. A random number $r = 1$ is chosen such that $0 < r < M$.
3. The ciphertext is: $c = \bar{g}^m r^M \bmod M^2 = 8^3 1^{221} \bmod 221^2 = 512$.

Decryption:

1. The ciphertext to be decrypted is $c = 512$.
2. The message is $m = \bar{L}(512^{48} \bmod 221^2)172 \bmod 221 = 3$

2.5. Quantization

To use the Paillier cryptosystem, data to be encrypted must be in the form of natural numbers in $\mathbb{Z}_M$. However, the signal values before encryption are in floating-point. Consequently, we employ quantization, mapping the floating-point numbers into $\mathbb{Z}_M$ (Darup et al., 2017). Using a signed fixed-point binary representation, we create a set, $\mathbb{Q}_{l_1,d}$, with parameters l_1 and d. These parameters define the total bit count (integer and fractional) and the fractional bits, respectively. The $\mathbb{Q}_{l_1,d}$ set encompasses rational numbers from -2^{l_1-d-1} to $2^{l_1-d-1} - 2^{-d}$, separated by 2^{-d}. A rational number q in $\mathbb{Q}_{l_1,d}$ can be expressed as $q \in \mathbb{Q}_{l_1,d}$, where $\exists \beta \in \{0,1\}^{l_1}$, and $q = -2^{l_1-d-1}\beta_{l_1} + \sum_{i=1}^{l_1-1} 2^{i-d-1}\beta_i$. To map a real number data point a to the $\mathbb{Q}_{l_1,d}$ set, we use the function $g_{l_1,d}$, defined by the equation,

$$\begin{aligned} &g_{l_1,d} : \mathbb{R} \to \mathbb{Q}_{l_1,d} \\ &g_{l_1,d}(a) := arg \min_{q \in \mathbb{Q}_{l_1,d}} |a - q| \end{aligned} \tag{7}$$

Next, the quantized data is transformed into a set of integers through a one-to-one (bijective) mapping known as $f_{l_2,d}$, as outlined in Darup et al. (2017). The following mapping ensures that the quantized data is transformed into a subset of the message space $\mathbb{Z}_M$:

$$\begin{aligned} &f_{l_2,d} : \mathbb{Q}_{l_1,d} \to \mathbb{Z}_{2^{l_2}} \\ &f_{l_2,d}(q) := 2^d q \ mod \ 2^{l_2} \end{aligned} \tag{8}$$

During the encryption process, integer plaintext messages from the set $Z_{2^{l_2}}$ are converted to ciphertexts, which can be decrypted back into the same set $Z_{2^{l_2}}$. To recover the original data from the set $\mathbb{Q}_{l_1,d}$, an inverse mapping, denoted as $f^{-1}_{l_2,d}$, is defined as follows:

$$f^{-1}_{l_2,d} : \mathbb{Z}_{2^{l_2}} \rightarrow \mathbb{Q}_{l_1,d} \tag{9}$$

$$f^{-1}_{l_2,d}(m) := \frac{1}{2^d}\begin{cases} m - 2^{l_2} & \text{if } m \geq 2^{l_2-1} \\ m & \text{otherwise} \end{cases} \tag{10}$$

3. Development of the encrypted decentralized control architecture

In this section, we describe the design of the encrypted decentralized control architecture, establish bounds on the errors in the encrypted decentralized control structure through a stability analysis, and formulate the predictor feedback-based decentralized LMPC.

3.1. Design of the encrypted decentralized control architecture

In the encrypted decentralized control architecture, depicted in Fig. 1, at time t_k, where k represents the sampling instance, signals $x(t_k)$ from sensors are encrypted to ciphertext c using the public key and transmitted to each control subsystem, within its respective edge computing unit. Within each unit, the encrypted signals are decrypted using the private key, and the quantized states $\hat{x}(t_k)$ are used to initialize the predictor in the j^{th} control subsystem, where j ranges from 1 to N_{sys}. The predictor computes the states after the input delay period, $\hat{x}(t_k + d_2)$. This is used to initialize the nonlinear process model of the j^{th} MPC. Subsequently, the j^{th} MPC computes the optimized control input trajectory along the whole prediction horizon and encrypts the control input $u_j(t_k + d_2)$. At the actuator, the ciphertext $\acute{c}$ is decrypted to the quantized input $\hat{u}(t_k + d_2)$. However, due to the input delay, d_2, the control input applied to the process by the actuator is $\hat{u}(t_k)$, which was calculated at time $t_k - d_2$. Since the data received and transmitted by the edge computers through the network remains encrypted, cybersecurity is ensured in the presence of secure edge computers.

The closed-loop design of Fig. 1 introduces two sources of error: one from state quantization in the sensor–controller link and another from control input quantization in the controller–actuator link. These errors are bounded by:

$$|x(t_k) - \hat{x}(t_k)| \leq 2^{-d-1} \tag{11a}$$

$$|u(t_k) - \hat{u}(t_k)| \leq 2^{-d-1} \tag{11b}$$

The derivation of the upper bounds of the quantization error in Eq. (11) has been explained in Remark 3. An additional error arises in the applied control input as the predictor, $\phi(x, u)$, receives $\hat{x}$ instead of the true state x to predict the states after the input delay period. Using the local Lipschitz property, this error will be confined by the underlying equation, where $L_1^{'} > 0$:

$$|\phi(\hat{x}, u) - \phi(x, u)| \leq L_1^{'}|\hat{x} - x| \leq L_1^{'}2^{-d-1} \tag{12}$$

Remark 2. In this work, a decentralized MPC, without inter-controller communication, is proposed to reduce the computational time and complexity of a centralized control problem. For possibly superior performance, some level of communication between controllers in different subsystems may be necessary to account for coupling effects between subsystems in large-scale processes. To establish this, a distributed control architecture could be used. However, encrypting-decrypting control input trajectories multiple times within a single sampling period could significantly increase the communication overhead due to encryption. To avoid this, a secure Ethernet crossover cable connection could be established between different computing units in a single control room responsible for computing all the control inputs of a particular process. This would avoid the need for encrypting-decrypting control inputs as their transmission would be secure, and encryption could still be used for signals transmitted to and from the control room.

Remark 3. Quantization error arises when the value to be quantized is not found exactly in the set $\mathbb{Q}_{l_1,d}$. The elements in this set are separated by 2^{-d}. Let us assume the value to be quantized is a, which lies between b and $b + 2^{-d}$. If the absolute difference between a and b is less than that between a and $b + 2^{-d}$, a is mapped to b, while, otherwise, a is mapped to $b + 2^{-d}$. Thus, the maximum potential difference between the actual value and the quantized value is half of the resolution or 2^{-d-1}. Further, this bound implies that a higher value of d would result in a smaller error due to quantization.

3.2. Decentralized LMPC

To reduce the computational time and complexity of a centralized control problem, we formulate a decentralized LMPC system as follows:

$$\mathscr{J}_j = \min_{u_{d_j} \in S(\Delta)} \int_{t_k}^{t_{k+N}} L_j(\tilde{x}_j(t), u_{d_j}(t))\, dt \tag{13a}$$

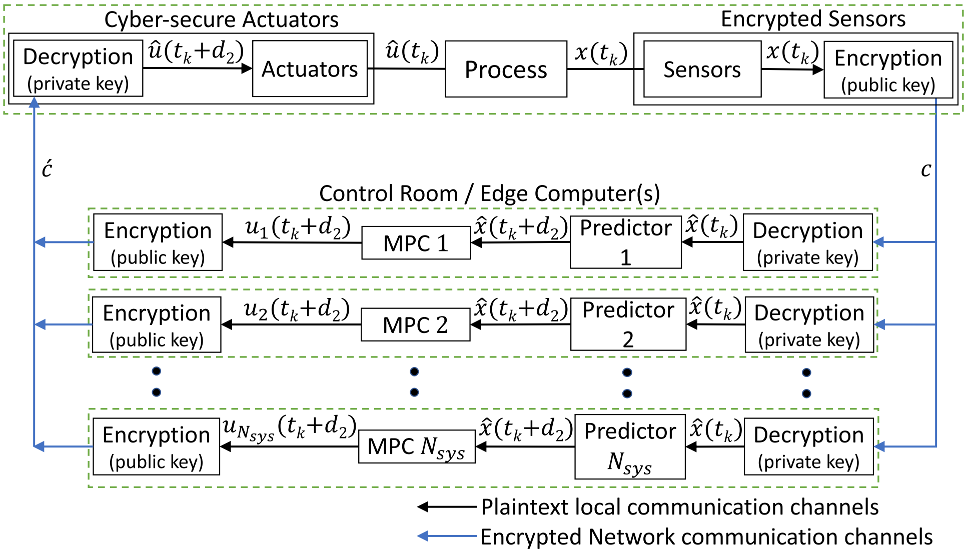

Fig. 1. Illustration of the encrypted decentralized control structure.

$$\text{s.t. } \dot{\tilde{x}}_j(t) = F_j(\tilde{x}(t), u_{d_j}(t)) \tag{13b}$$

$$u_{d_j}(t) \in U_j, \quad \forall\, t \in [t_k, t_{k+N}) \tag{13c}$$

$$\tilde{x}(t_k) = \hat{x}(t_k) \tag{13d}$$

$$\begin{aligned}&\dot{V}(\hat{x}(t_k), u_{d_j}(t_k)) \le \dot{V}(\hat{x}(t_k), \Phi_j(\hat{x}(t_k))),\\ &\quad \text{if } \hat{x}(t_k) \in \Omega_\rho \backslash \Omega_{\rho_{\min}}\end{aligned} \tag{13e}$$

$$V(\tilde{x}(t)) \le \rho_{min}, \quad \forall\, t \in [t_k, t_{k+N}),\ \text{if } \hat{x}(t_k) \in \Omega_{\rho_{\min}} \tag{13 f}$$

Each LMPC has access to full-state feedback measurements but only takes into account the dynamics of its respective subsystem. Consequently, we develop separate first-principles-based models for each subsystem j where $j = 1, \ldots, N_{sys}$, to predict the states x_j and compute the control input u_{d_j} to be applied by the corresponding actuators within the j^{th} subsystem. $\tilde{x}_j$ represents the predicted state trajectory of the process model of the j^{th} LMPC. The quantized states, $\hat{x}$, serve as the initial conditions for the LMPC process model to predict the state trajectory as per Eq. (13b), which is used to integrate the cost function of Eq. (13a) to calculate optimized control inputs, $u^*{}_{d_j}(t|t_k)$, for the entire prediction horizon. However, the LMPC transmits only the first input of this sequence to the actuator for application to the system within the interval $t \in [t_k, t_{k+1})$ and repeats this process at each sampling period. k is the sampling instance, and N represents the number of sampling periods within the prediction horizon. Eq. (13c) represents the constraints imposed on the control inputs, and Eq. (13d) uses the quantized states to initialize the plant model described in Eq. (13b). The Lyapunov constraint in Eq. (13e) ensures that, if the state $x(t_k)$ at time t_k lies within the set $\Omega_\rho \backslash \Omega_{\rho_{\min}}$, where $\rho_{\min}$ represents a level set of V in proximity to the origin, the time-derivative of the control Lyapunov function of the closed-loop subsystem j under the j^{th} LMPC is less than or equal to the time-derivative of the control Lyapunov function when the subsystem is controlled by the stabilizing controller $\Phi_j(x)$. When the closed-loop state $x(t_k)$ enters $\Omega_{\rho_{\min}}$, the constraint of Eq. (13f) ensures that this state remains within $\Omega_{\rho_{\min}}$.

3.3. *Robustness of the encrypted decentralized LMPC to time-delay systems*

In this subsection, we will focus on the closed-loop stability analysis of the perturbed nonlinear system of Eq. (3), taking into consideration sufficiently small state delays only (i.e., $d_2 \equiv 0$ and $d_1 > 0$). However, the stabilization of the perturbed system of Eq. (3) in the presence of both state and input delays will be achieved using an encrypted decentralized LMPC with predictor feedback in Section 3.4. We first establish stability of the closed-loop system under the encrypted stabilizing controller $\hat{\Phi}(\hat{x})$, followed by extending our analysis to stability of the system under the encrypted decentralized LMPC system introduced in the previous section.

Theorem 1. Considering the system of Eq. (3) under the encrypted stabilizing controller $\hat{\Phi}(\hat{x})$, we examine the stability of the time-delay system without any input delay (i.e., $d_2 \equiv 0$ and $d_1 > 0$). The stabilizing controller $\Phi(x)$, without encryption and delays, adheres to the inequalities outlined in Eq. (4). Furthermore, we assume that the initial state x_0 resides within the region $\Omega_{\hat{\rho}}$ where $\hat{\rho} < \rho$. Given a sufficiently large time $T > 0$, where T is the time needed for $x(t)$ to enter $\Omega_{\rho_{\min}}$, we can determine positive real numbers $L_x^{'}, L_\xi^{'}, L_q^{'}, M_F, M_{d_1}$, and $e_t = (L_1 + 1)2^{-d-1}$, for which there exist Δ, d_1, d, and $\epsilon_w > 0$, such that the following conditions are satisfied:

$$\begin{aligned}&L_x^{'} M_F \Delta + L_\xi^{'} M_{d_1} d_1 + L_q^{'} \left|e_t\right| - \frac{c_3}{c_2}\rho_s \le -\epsilon_w\\ &\rho_{min} = max\{V(x(t+\Delta))|V(x(t)) \le \rho_s\}\end{aligned} \tag{14}$$

where $\hat{\rho} > \rho_{\min} > \rho_s$. Then, the closed-loop state $x(t)$ under the encrypted stabilizing controller remains bounded in $\Omega_{\hat{\rho}}$ and is ultimately bounded in $\Omega_{\rho_{\min}}$ for $t \ge T$. **Proof.** This proof is divided into four parts. First, we will establish bounds on the error due to quantization in the time-delay system under the encrypted stabilizing controller, keeping the input delay, $d_2 \equiv 0$. Then, we will establish bounds for the error due to state delays, followed by limiting the error due to the control input being applied in a sample-and-hold manner. Lastly, based on these bounds, we can determine the positive constants $L_x^{'}, L_\xi^{'}, L_q^{'}, M_F, M_{d_1}$, and $e_t = (L_1 + 1)2^{-d-1}$, for which there exist Δ, d_1, d, and $\epsilon_w > 0$, such that the state of the closed-loop system from any initial condition $x_0 \in \Omega_{\hat{\rho}} \backslash \Omega_{\rho_s}$ converges within $\Omega_{\rho_{\min}}$ within time T. Under the encrypted stabilizing controller, the control input $u(t)$ can be written as $u(t) = \hat{\Phi}(\hat{x}(t_k))$. Substituting this in the nonlinear system of Eq. (3) without any input delay (i.e. $d_2 \equiv 0$), the time-derivative of the control Lyapunov function can be written as:

$$\dot{V} = \frac{\partial V(x(t))}{\partial x} f(x(t), x(t) + \xi_1(t), \hat{\Phi}(\hat{x}(t_k))) \tag{15}$$

Based on the error bounds resulting from quantization, as derived in Eq. (11), $\hat{\Phi}(\hat{x}(t_k)) \le \Phi(\hat{x}(t_k)) + 2^{-d-1}$,

$$\begin{aligned}\dot{V} \quad &\le \frac{\partial V(x(t))}{\partial x} f\left(x(t), x(t) + \xi_1(t), \Phi(\hat{x}(t_k)) + 2^{-d-1}\right)\\ &\le \frac{\partial V(x(t))}{\partial x} f(x(t), x(t) + \xi_1(t), \Phi(\hat{x}(t_k)) - \Phi(x(t_k)) + \Phi(x(t_k)) + e_t)\end{aligned} \tag{16}$$

using $\Phi(\hat{x}(t_k)) - \Phi(x(t_k)) \le L_1 |\hat{x} - x| \le L_1 2^{-d-1}$ in Eq. (16):

$$\begin{aligned}\dot{V} \quad &\le \frac{\partial V(x(t))}{\partial x} f\left(x(t), x(t) + \xi_1(t), \Phi(x(t_k)) + (L_1+1)2^{-d-1}\right)\\ &\le \frac{\partial V(x(t))}{\partial x} f(x(t), x(t) + \xi_1(t), \Phi(x(t_k)) + e_t)\end{aligned} \tag{17}$$

where $e_t = (L_1 + 1)2^{-d-1}$ represents the error due to quantization. Using the constraints outlined in Eq. (4), Eq. (17) can be re-written as:

$$\begin{aligned}\dot{V} \quad &\le \frac{\partial V(x(t))}{\partial x} f(x(t), x(t) + \xi_1(t), \Phi(x(t_k)) + e_t)\\ &- \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), x(t_k), \Phi(x(t_k)))\\ &+ \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), x(t_k), \Phi(x(t_k))) \le \frac{\partial V(x(t))}{\partial x} f(x(t), x(t) + \xi_1(t), \Phi(x(t_k))\\ &+ e_t) - \frac{\partial V(x(t_k))}{\partial x} f(x(t_k), x(t_k), \Phi(x(t_k))) - c_3 |x(t_k)|^2\end{aligned} \tag{18}$$

Based on Eq. (18), we can define the following: $g(x, \xi_1, e_t) = f(x, x + \xi_1, \Phi(x) + e_t)$. In addition, there exist positive constants, $L_x^{'}$, $L_\xi^{'}$, and $L_q^{'}$ such that the following Lipschitz inequality holds for all $x, x' \in \Omega_{\hat{\rho}}$:

$$\left|\frac{\partial V(x)}{\partial x} g(x, \xi_1, e_t) - \frac{\partial V(x')}{\partial x} g(x', 0, 0)\right| \le L_x^{'}|x - x'| + L_\xi^{'}|\xi_1| + L_q^{'}|e_t| \tag{19}$$

Thus, Eq. (18) can be re-written as:

$$\begin{aligned}\dot{V} \quad &\le \quad \frac{\partial V(x(t))}{\partial x} g(x(t), \xi_1(t), e_t) \quad - \quad \frac{\partial V(x(t_k))}{\partial x} g(x(t_k), 0, 0)\\ &\qquad - c_3 |x(t_k)|^2\\ &\le \quad L_x^{'}|x(t) - x(t_k)| + L_\xi^{'}|\xi_1(t)| + L_q^{'}|e_t| - c_3|x(t_k)|^2\end{aligned} \tag{20}$$

The upper bound of the perturbation term ξ_1 due to state delays can be represented as:

$$|\xi_1(t)| = |x(t-d_1) - x(t)| \le d_1 M_{d_1} \tag{21}$$

where $M_{d_1} = \max\limits_{s\in[-d_1,0]} \left|x(t+\ s)\right|, \forall t \in [0,\ T]$. Substituting the bound on $|\xi_1(t)|$ derived from Eq. (21), we obtain:

$$\dot{V} \le L_x^{'}|x(t) - x(t_k)| + L_\xi^{'} d_1 M_{d_1} + L_q^{'}|e_t| - c_3|x(t_k)|^2 \tag{22}$$

Due to the continuity of $x(t)\ \forall\ t \in [t_k,\ t_k + \Delta)$, we can write that $|x(t) - x(t_k)| \le M_F\Delta,\ \forall\ t \in [t_k,\ t_k + \Delta)$. Using this bound and the inequalities of Eq. (4), it follows from Eq. (22):

$$\dot{V} \le L_x^{'} M_F \Delta + L_\xi^{'} d_1 M_{d_1} + L_q^{'}|e_t| - \frac{c_3}{c_2}\rho_s \tag{23}$$

In the above equation, the first term represents the error due to sample-and-hold implementation of the control input, the second term represents the error due to state delays, and the third term represents the error due to quantization. All these errors are bounded and can be made sufficiently small by constraining the sampling time and state delay to be sufficiently small, and using a higher quantization parameter d for encryption. Therefore, their sum is also bounded and can be made sufficiently small. This implies that, for the chosen time T, there exist positive real numbers Δ, d_1, d, and ϵ_w, such that the following inequality holds $\forall\ t \in [0,T]$:

$$L_x^{'} M_F \Delta + L_\xi^{'} d_1 M_{d_1} + L_q^{'}|e_t| - \frac{c_3}{c_2}\rho_s \le -\epsilon_w$$

which implies that $\dot{V} \le -\epsilon_w$ for any $x(t_k) \in \Omega_{\hat{\rho}} \backslash \Omega_{\rho_s}$ for all $t_k \in [0,\ T]$. This establishes that, if the conditions of Eq. (14) are met, the closed-loop system state under the encrypted stabilizing controller is always bounded in $\Omega_{\hat{\rho}}$ and converges to $\Omega_{\rho_s} \subseteq \Omega_{\rho_{\min}}$ within time T, and remains there. Below, we proceed with the stability proof of the closed-loop system under the encrypted decentralized MPC.

Theorem 2. Considering the system of Eq. (3) under the encrypted decentralized LMPC of Eq. (13), we examine the stability of the time-delay system without any input delay (i.e., $d_2 \equiv 0$ and $d_1 > 0$). We assume that the initial state x_0 resides within the region $\Omega_{\hat{\rho}}$. Given a sufficiently large time $T > 0$, where T is the time needed for $x(t)$ to enter $\Omega_{\rho_{\min}}$, we extend the results obtained in Theorem 1 to the encrypted decentralized LMPC of Eq. (13) maintaining our previous assumption that $\widehat{\rho} > \rho_{\min} > \rho_s$. Then, if the following conditions are satisfied,

$$\begin{aligned} \dot{V} \quad &\le \quad L_x^{'} M_F \Delta + L_\xi^{'} d_1 M_{d_1} + L_q^{'}|e_t| - \frac{c_3}{c_2}\rho_s \le -\epsilon_w \\ \rho_{\min} \quad &= \quad \max\{V(x(t+\Delta))|V(x(t)) \le \rho_s\} \end{aligned} \tag{24}$$

the closed-loop state $x(t)$ remains bounded in $\Omega_{\hat{\rho}}$ and is ultimately bounded in $\Omega_{\rho_{\min}}$ for $t \ge T$, under the proposed encrypted decentralized LMPC of Eq. (13). **Proof.** Firstly, within this proof, we establish the recursive feasibility of the optimization problem within each decentralized LMPC. Subsequently, under the optimized control actions of the encrypted decentralized LMPC of Eq. (13), we will prove the boundedness and convergence of the closed-loop state of the nonlinear system within the set $\Omega_{\hat{\rho}}$, extending the results of Theorem 1. Initially, we consider $x(t) \in \Omega_{\hat{\rho}} \backslash \Omega_{\rho_{\min}}$. The input trajectories $\widehat{\Phi}_j(\widetilde{x}(t_k)),\quad j = 1, \ldots, N_{sys}$ for $t \in [t_k,\ t_{k+1})$ are feasible solutions to the optimization problem outlined in Eq. (13), as the input constraint of Eq. (13c) and the Lyapunov constraint of Eq. (13e) are both satisfied. Then, we consider $x(t) \in \Omega_{\rho_{\min}}$. The input trajectories $\widehat{\Phi}_j(\widetilde{x}(t_{k+i})),\quad i = 0, 1, \ldots, N-1,\quad j = 1, \ldots, N_{sys}$ for $t \in [t_k,\ t_{k+N})$ satisfy the constraints on the inputs in Eq. (13c) and the Lyapunov-based constraint of Eq. (13f). It has been proven in Theorem 1 that the states predicted by the LMPC process model of Eq. (13b) can remain within $\Omega_{\rho_{\min}}$ under the encrypted stabilizing controllers $\widehat{\Phi}_j(\widetilde{x})$ for time $t \ge T$. Thus, the optimization problem of each decentralized LMPC would be feasible for all $x_0 \in \Omega_{\hat{\rho}}$ and can be solved by recursive feasibility for $t \in [t_k,\ t_{k+1})$, i.e.,

$$\begin{aligned} &\frac{\partial V(x(t))}{\partial x_j} f_j(x(t), x(t) + \xi_1(t), \widehat{u}_{d_j}(t_k)) \\ &\le \frac{\partial V(x(t))}{\partial x_j} f_j\big(x(t), x(t) + \xi_1(t), \widehat{\Phi}_j(\widehat{x}(t_k))\big), \quad \forall j = 1, \ldots, N_{sys} \end{aligned} \tag{25}$$

The control Lyapunov function for the overall system $V(x)$ may take the form of a linear combination of control Lyapunov functions for individual subsystems. In this representation, $V(x)$ is expressed as the sum of $V_j(x_j)$ for each subsystem, where V_j is assumed to be a function of x_j only. The time-derivative of the control Lyapunov function of the encrypted decentralized LMPC can be expressed as follows:

$$\dot{V} = \sum_{j=1}^{N_{sys}} \frac{\partial V(x(t))}{\partial x_j} f_j(x(t), x(t) + \xi_1(t), \widehat{u}_{d_j}(t_k)) \tag{26}$$

Based on the Lyapunov constraint, the following inequality holds:

$$\begin{aligned} \dot{V} \quad &= \quad \sum_{j=1}^{N_{sys}} \frac{\partial V(x(t))}{\partial x_j} f_j(x(t), x(t) + \xi_1(t), \widehat{u}_{d_j}(t_k)) \\ &\le \sum_{j=1}^{N_{sys}} \frac{\partial V(x(t))}{\partial x_j} f_j\big(x(t), x(t) + \xi_1(t), \widehat{\Phi}_j(\widehat{x}(t_k))\big) \end{aligned} \tag{27}$$

From Eq. (26) and Eq. (27), the time-derivative of the control Lyapunov function under the encrypted decentralized LMPC satisfies the inequality,

$$\frac{\partial V(x(t))}{\partial x} f(x(t), x(t) + \xi_1(t), \widehat{u}_d(t_k)) \le \frac{\partial V(x(t))}{\partial x} f(x(t), x(t) + \xi_1(t), \widehat{\Phi}(\widehat{x}(t_k))) \tag{28}$$

However, from the results of Theorem 1 (Eq. (23)), it follows that the right-hand side of Eq. (28) is bounded as follows:

$$\begin{aligned} \frac{\partial V(x(t))}{\partial x} f(x(t), x(t) + \xi_1(t), \widehat{u}_d(t_k)) &\le L_x^{'} M_F \Delta + L_\xi^{'} d_1 M_{d_1} + L_q^{'}|e_t| - \frac{c_3}{c_2}\rho_s \\ &\le -\epsilon_w \end{aligned} \tag{29}$$

Thus, for the chosen time T, there exist positive real numbers Δ, d_1, d, and ϵ_w, such that the following inequality holds $\forall\ t \in [0,T]$,

$$L_x^{'} M_F \Delta + L_\xi^{'} d_1 M_{d_1} + L_q^{'}|e_t| - \frac{c_3}{c_2}\rho_s \le -\epsilon_w$$

which implies that $\dot{V} \le -\epsilon_w$ for any $x(t_k) \in \Omega_{\hat{\rho}} \backslash \Omega_{\rho_s}$ for all $t_k \in [0,\ T]$. This establishes that, if the conditions of Eq. (24) are met, the closed-loop system state is always bounded in $\Omega_{\hat{\rho}}$, and it converges to $\Omega_{\rho_s} \subseteq \Omega_{\rho_{\min}}$ within time T, and remains there. This completes the proof for the stability of the system under the encrypted decentralized LMPC.

Remark 4. As discussed in Section 3.3, we employ the predictor feedback methodology outlined in Section 3.4 to achieve system stabilization in the presence of input delays. The stability analysis does not consider the perturbation caused by input delays. However, a similar approach to the one used to establish bounds on state delays, as demonstrated in Eq. (21), could be employed to account for the influence of input delays. Incorporating input delay perturbations into the proof would establish a very stringent upper limit on the allowable value of d_2, rendering the proof valid only for relatively small input delays. As outlined in Eq. (3), the perturbation resulting from input delays can be expressed as $\xi_2(t) = u(t - d_2) - u(t)$. Consequently, it becomes evident that, as d_2 approaches zero, $\xi_2(t)$ tends to zero as well. In the interest of maintaining a more generalized analysis with established bounds applicable even to substantial input delays, we have chosen to omit this consideration from the proof. Instead, we opt to address input delay challenges by employing a predictor, ensuring the validity of our analysis across a broader range of scenarios.

3.4. Predictor feedback decentralized LMPC methodology

This subsection formulates a predictor feedback-based decentralized LMPC for the nonlinear system described in Eq. (1). A first-principles-based state predictor is integrated in the closed-loop system to compensate for the effect of input delays. At time t_k, where k is the sampling instance, the predictor of the j^{th} subsystem receives the quantized states $\hat{x}(t_k)$. It uses the control input trajectory $u_{d_j}(t)$ computed previously by the j^{th} LMPC, and estimates the control inputs for the other subsystems using the stabilizing control law, $\Phi(x)$, over t_k to $t_k + d_2$, to predict the state values of the entire system at $t_k + d_2$. Additionally, the LMPCs employ a DDE-based nonlinear process model specific to their subsystem. Thus, the predictor also transmits values of the states from time $t_k + d_2 - d_1$ to $t_k + d_2$, which are used by the DDE model to account for the state delays in the system. Within a decentralized control framework, where inter-controller communication is absent, the predictor of the j^{th} subsystem only has access to the control inputs computed by the j^{th} LMPC. Thus, an estimate of the control inputs of the other subsystems can be made through the stabilizing control law, utilizing state feedback. The inputs are assumed to be at their steady state values from time 0 to d_2. The j^{th} LMPC is then initialized with the shifted timescale $\bar{t}_k = t_k + d_2$ to calculate the optimal control input trajectory, u_{d_j}, from $\bar{t}_k$ to $\bar{t}_{k+N}$. The LMPC formulation with the shifted time scale is described as follows:

$$\mathcal{J}_j = \min_{u_{d_j} \in S(\Delta)} \int_{\bar{t}_k}^{\bar{t}_{k+N}} L_j(\tilde{x}_j(t), u_{d_j}(t))\, \mathrm{d}t \tag{30a}$$

$$\text{s.t. } \dot{\tilde{x}}_j(t) = F_j(\tilde{x}(t), u_{d_j}(t)) \tag{30b}$$

$$u_{d_j}(t) \in U_j, \quad \forall\, t \in [\bar{t}_k, \bar{t}_{k+N}) \tag{30c}$$

$$\tilde{x}(\bar{t}_k) = \hat{x}(\bar{t}_k) \tag{30d}$$

$$\begin{aligned} &\dot{V}(\hat{x}(\bar{t}_k), u_{d_j}(\bar{t}_k)) \le \dot{V}(\hat{x}(\bar{t}_k), \Phi_j(\hat{x}(\bar{t}_k))), \\ &\text{if } \hat{x}(\bar{t}_k) \in \Omega_\rho \backslash \Omega_{\rho_{\min}} \end{aligned} \tag{30e}$$

$$\begin{aligned} &V(\tilde{x}(t)) \le \rho_{\min}, \quad \forall\, t \in [\bar{t}_k, \bar{t}_{k+N}), \\ &\text{if } \hat{x}(\bar{t}_k) \in \Omega_{\rho_{\min}} \end{aligned} \tag{30 f}$$

Remark 5. As mentioned earlier in Section 3.3, we employ the predictor feedback methodology outlined in Section 3.4 to achieve system stabilization in the presence of input delays. In the absence of a predictor, nominal to modest input delays can lead to an oscillatory convergence of the closed-loop system states around their respective steady states within Ω_ρ but outside $\Omega_{\rho_{\min}}$, while larger input delays can cause the state to exit Ω_ρ. However, with a predictor feedback methodology, the closed-loop states can be stabilized within $\Omega_{\rho_{\min}}$ even under large input delays. This is demonstrated in the example described in Section 4.

4. Application to a nonlinear chemical process network operating at an unstable steady state

This section demonstrates the proposed encrypted decentralized control architecture on a nonlinear chemical process network with input and state delays, operating at an unstable steady state. A nonlinear dynamical model based on first-principles modeling fundamentals is developed for the state predictor and the LMPCs. This model is partitioned into N_{sys} subsystems to construct first-principles-based process models of the decentralized LMPC of each subsystem. Guidelines are established to implement the encrypted decentralized LMPC system in any nonlinear process with delays. We then conduct closed-loop simulations, employing the decentralized LMPC with and without the predictor feedback, and analyze the results.

4.1. Process description and model development

The process considered is the synthesis of ethylbenzene (EB) by reacting ethylene (E) and benzene (B) within two non-isothermal, well-mixed continuous stirred tank reactors (CSTRs) as depicted in Fig. 2. The primary reaction, termed as “primary”, is characterized as a second-order, exothermic, and irreversible reaction, in conjunction with two supplementary side reactions. The chemical reactions taking place are articulated as follows:

$$C_2H_4 + C_6H_6 \rightarrow C_8H_{10} \qquad \text{(primary)} \tag{31a}$$

$$C_2H_4 + C_8H_{10} \rightarrow C_{10}H_{14} \tag{31b}$$

$$C_6H_6 + C_{10}H_{14} \rightarrow 2C_8H_{10} \tag{31c}$$

Details of the steady-state values and model parameter values can be obtained from Kadakia et al. (2023). The dynamic model of the initial CSTR is described by the following mass and energy balance equations:

$$\dot{C}_{E_1}(t) = \frac{F_1 C_{Eo_1}(t - d_2) - F_{out_1} C_{E_1}(t)}{V_1} - r_{1,1} - r_{1,2} \tag{32a}$$

$$\dot{C}_{B_1}(t) = \frac{F_1 C_{Bo_1}(t - d_2) - F_{out_1} C_{B_1}(t)}{V_1} - r_{1,1} - r_{1,3} \tag{32b}$$

$$\dot{C}_{EB_1}(t) = \frac{-F_{out_1} C_{EB_1}(t)}{V_1} + r_{1,1} - r_{1,2} + 2r_{1,3} \tag{32c}$$

$$\dot{C}_{DEB_1}(t) = \frac{-F_{out_1} C_{DEB_1}(t)}{V_1} + r_{1,2} - r_{1,3} \tag{32d}$$

$$\begin{aligned} \dot{T}_1(t) \;=\; &\frac{T_{1_o} F_1 - T_1(t) F_{out_1}}{V_1} + \sum_{j=1}^{3} \frac{-\Delta H_j}{\rho_1 C_p} r_{1,j} \\ &+ \frac{Q_1(t - d_2)}{\rho_1 C_p V_1} \end{aligned} \tag{32e}$$

The dynamic model of the second CSTR is represented by the following equations:

$$\begin{aligned} \dot{C}_{E_2}(t) = &\frac{F_2 C_{Eo_2}(t - d_2) + F_{out_1} C_{E_1}(t - d_1)}{V_2} \\ &- \frac{F_{out_2} C_{E_2}(t)}{V_2} - r_{2,1} - r_{2,2} \end{aligned} \tag{33a}$$

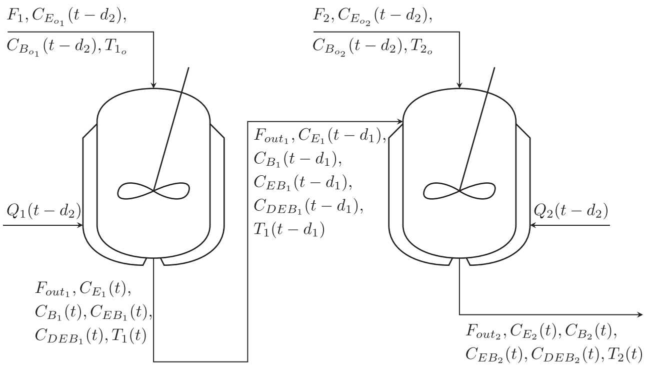
$F_1, C_{E_{o_1}}(t - d_2),$
$C_{B_{o_1}}(t - d_2), T_{1_o}$
$F_2, C_{E_{o_2}}(t - d_2),$
$C_{B_{o_2}}(t - d_2), T_{2_o}$
$Q_1(t - d_2)$
$F_{out_1}, C_{E_1}(t - d_1),$
$C_{B_1}(t - d_1),$
$C_{EB_1}(t - d_1),$
$C_{DEB_1}(t - d_1),$
$T_1(t - d_1)$
$Q_2(t - d_2)$
$F_{out_1}, C_{E_1}(t),$
$C_{B_1}(t), C_{EB_1}(t),$
$C_{DEB_1}(t), T_1(t)$
$F_{out_2}, C_{E_2}(t), C_{B_2}(t),$
$C_{EB_2}(t), C_{DEB_2}(t), T_2(t)$

Fig. 2. Process schematic featuring two CSTRs connected in series.

$$\dot{C}_{B_2}(t) = \frac{F_2 C_{Bo_2}(t-d_2) + F_{out_1} C_{B_1}(t-d_1)}{V_2} - \frac{F_{out_2} C_{B_2}(t)}{V_2} - r_{2,1} - r_{2,3} \tag{33b}$$

$$\dot{C}_{EB_2}(t) = \frac{F_{out_1} C_{EB_1}(t-d_1) - F_{out_2} C_{EB_2}(t)}{V_2} + r_{2,1} - r_{2,2} + 2r_{2,3} \tag{33c}$$

$$\dot{C}_{DEB_2}(t) = \frac{F_{out_1} C_{DEB_1}(t-d_1) - F_{out_2} C_{DEB_2}(t)}{V_2} + r_{2,2} - r_{2,3} \tag{33d}$$

$$\dot{T}_2(t) = \frac{T_{2_o} F_2 + T_1(t-d_1) F_{out_1} - T_2(t) F_{out_2}}{V_2} + \sum_{j=1}^{3} \frac{-\Delta H_j}{\rho_2 C_p} r_{2,j} + \frac{Q_2(t-d_2)}{\rho_2 C_p V_2} \tag{33e}$$

where the reaction rates are calculated by the following expressions:

$$r_{i,1} = k_1 e^{\frac{-E_1}{RT_i(t)}} C_{E_i}(t) C_{B_i}(t) \tag{34a}$$

$$r_{i,2} = k_2 e^{\frac{-E_2}{RT_i(t)}} C_{E_i}(t) C_{EB_i}(t) \tag{34b}$$

$$r_{i,3} = k_3 e^{\frac{-E_3}{RT_i(t)}} C_{DEB_i}(t) C_{B_i}(t) \tag{34c}$$

and $i = \{1,\ 2\}$ is the reactor index. The state variables are the concentration of ethylene, benzene, ethylbenzene, di-ethylbenzene, and the reactor temperature for each CSTR in deviation terms, that is: $x^\top = [C_{E_1} - C_{E_{1s}},\ C_{B_1} - C_{B_{1s}},\ C_{EB_1} - C_{EB_{1s}},\ C_{DEB_1} - C_{DEB_{1s}},\ T_1 - T_{1s},\ C_{E_2} - C_{E_{2s}},\ C_{B_2} - C_{B_{2s}},\ C_{EB_2} - C_{EB_{2s}},\ C_{DEB_2} - C_{DEB_{2s}},\ T_2 - T_{2s}]$ The subscript, *s,* denotes the steady-state value. The state delay, representing the time needed to transport the output of the initial CSTR to the second CSTR, is set at $d_1 = 0.5$ min. The rate of heat removal for the two reactors $[Q_1 - Q_{1s},\ Q_2 - Q_{2s}]$ and inlet feed concentrations for each reactor, $[C_{E_{o1}} - C_{E_{o1s}}, C_{B_{o1}} - C_{B_{o1s}}, C_{E_{o2}} - C_{E_{o2s}}, C_{B_{o2}} - C_{B_{o2s}}]$, are the manipulated inputs with input delay $d_2 = 1$ min. These inputs are bounded by the closed sets, $[-10^4,\ 2\times10^3]$ kW, $[-1.5\times10^4,\ 5\times10^3]$ kW, $[-2.5,\ 2.5]$ kmol/m^3, $[-2.5,\ 2.5]$ kmol/m^3, $[-3,\ 3]$ kmol/m^3, and $[-3,\ 3]$ kmol/m^3, respectively. To determine the stability of the chosen steady-state, an open loop simulation was performed where the control inputs were maintained at their steady state values, and the system states were initialized at a point close to their operating steady-state within $\Omega_{\rho_{\min}}$. After a finite duration of process time, the states exited the stability region, Ω_ρ, and converged to another steady state, implying that the chosen steady-state is an unstable one. Furthermore, the rationale for choosing this steady-state was its ability to provide a high steady-state concentration (4.22 kmol/m^3) of the desired product, ethyl benzene, at reasonable operating conditions, at the outlet of reactor 2, making it the economically optimal steady state to operate at.

We create two decentralized LMPCs in our design. The first LMPC (LMPC 1) utilizes the first-principles-based model specific to subsystem 1, which corresponds to the dynamic model of CSTR 1 (Eq. (32)), while the second LMPC (LMPC 2) employs a first-principles-based model specific to subsystem 2, which corresponds to the dynamic model of CSTR 2 (Eq. (33)). LMPC 1 does not require complete state feedback, given that the dynamics of its subsystem are entirely independent of subsystem 2. However, the evolution of the states within the second CSTR is influenced by the states of the first CSTR. Thus, LMPC 1 receives $x_1 = [C_{E_1} - C_{E_{1s}},\ C_{B_1} - C_{B_{1s}},\ C_{EB_1} - C_{EB_{1s}},\ C_{DEB_1} - C_{DEB_{1s}},\ T_1 - T_{1s}]^\top$ and optimizes the control inputs $u_1 = [C_{E_{o1}} - C_{E_{o1s}}, C_{B_{o1}} - C_{B_{o1s}}, Q_1 - Q_{1s}]^\top$. LMPC 2 receives full state feedback x, and optimizes the control inputs $u_2 = [C_{E_{o2}} - C_{E_{o2s}}, C_{B_{o2}} - C_{B_{o2s}}, Q_2 - Q_{2s}]^\top$. The control objective is to operate both CSTRs at their unstable equilibrium point through the encrypted decentralized control scheme, employing quantized states and inputs for computation and actuation.

4.2. Encrypting the decentralized control architecture

Before implementing encryption–decryption into a process, the selection of parameters, namely d, l_1, and l_2 is performed. Based on the extreme feasible states and inputs, the integer bit count $l_1 - d$ is derived. The upper limit in the $\mathbb{Q}_{l_1,d}$ set is obtained via the formula $2^{l_1-d-1} - 2^{-d}$, whereas the lower limit is -2^{l_1-d-1}. The choice of the quantization parameter d, representing the fractional bit count, rests on the desired accuracy and range of state and input values. Additionally, l_2 is chosen to exceed l_1. Accordingly, for the example in this section, $l_1 - d$ is calculated to be 16, from which l_1 and d are then fixed. Within the set $\mathbb{Q}_{l_1,d}$, rational numbers are separated by a resolution of 2^{-d}. For simulation purposes, we use, $d = 8$. For $d = 8$, $l_1 = 24$ and we select $l_2 = 30$. The Paillier Encryption procedure is implemented through Python's "phe" module, PythonPaillier (2013). For solving the constrained non-convex optimization problem in the LMPCs within the decentralized control structure, we leverage the Python module of the IPOPT software (Wächter and Biegler, 2006).

While deciding the sampling time (Δ) for an encrypted decentralized system, it is crucial to ensure that it exceeds the total time required for encryption–decryption of the states and control inputs, time required by the predictor to predict the states after the input delay, and the time needed to compute the control inputs at each sampling instance for the considered quantization parameter d, for any subsystem, as these computations would occur concurrently in different edge computing units. Mathematically,

$$\begin{aligned}\Delta \quad > \quad & \max(\text{Encryption-decryption time})_j \\ & + \max(\text{Control input computation time})_j \\ & + \max(\text{State-prediction time})_j\end{aligned} \tag{35}$$

where $j = \{1, \ldots, N_{sys}\}$ represents the control subsystem. Considering the above criteria, the sampling time Δ is chosen as 30 s in the discussed example.

To calculate the cost function of the LMPCs over the prediction horizon, the integration step $h_c = 10^{-2} \times \Delta$ is chosen. The positive definite matrix P in the control Lyapunov function $V = x^\top P x$ is selected as diag [250 500 500 1000 2.5 250 250 500 1000 2.5], from extensive simulations. The LMPCs employ a prediction horizon of $N = 3$ sampling periods. The stability criterion is defined as $\rho = 1000$, while $\rho_{\min} = 2$ is the smaller level set of the Lyapunov function where the state is desired to be confined. The weight matrices in the cost function of LMPCs are chosen as $Q_1 = \text{diag}$ [2000 2000 5000 5 50], $Q_2 = \text{diag}$ [1000 1000 2500 5 135], $R_1 = \text{diag}$ [1 1 5 × 10^{-6}], and $R_2 = \text{diag}$ [20 15 2.5 × 10^{-4}]. The cost function is defined as $L_j(x_j, u_j) = x_j^\top Q_j x_j + u_j^\top R_j u_j$ where $j = 1,\ 2$ represents the LMPC j. As di-ethylbenzene, the undesired product, is present in trace amounts in both CSTRs, its trajectories are not depicted.

4.3. Simulation results of the encrypted decentralized control architecture

The proposed encrypted decentralized control architecture is applied to a nonlinear chemical process with state and input delays. Figs. 3, 4 to 5 and 6, 7 to 8 depict the results for the encrypted decentralized LMPC system without and with predictor feedback, respectively.

In the absence of a predictor, the states and inputs of both CSTRs show considerable oscillations, as shown in Fig. 3 to 5. Additionally, the temperatures of both CSTRs overshoot their set-points. With the addition of the state predictor, the oscillations in both states and inputs are negligible as observed in Fig. 6 to 8. Furthermore, there is no overshoot of the temperature in CSTR 1, and the overshoot in temperature is decreased for CSTR 2. Moreover, the inclusion of the predictor enables us to achieve convergence of the states within the targeted stability region, denoted as $\Omega_{\rho_{\min}}$. This was not attainable solely with the encrypted

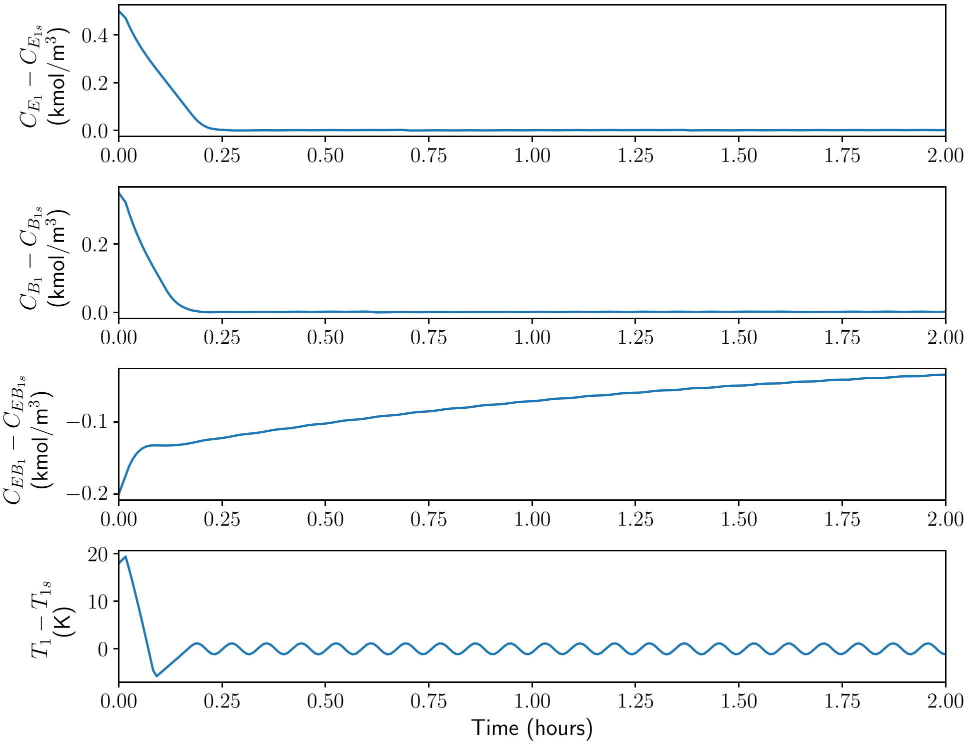

Fig. 3. State profiles of CSTR 1 under the encrypted decentralized LMPC for state delay $d_1 = 0.5$ min, and input delay $d_2 = 1$ min.

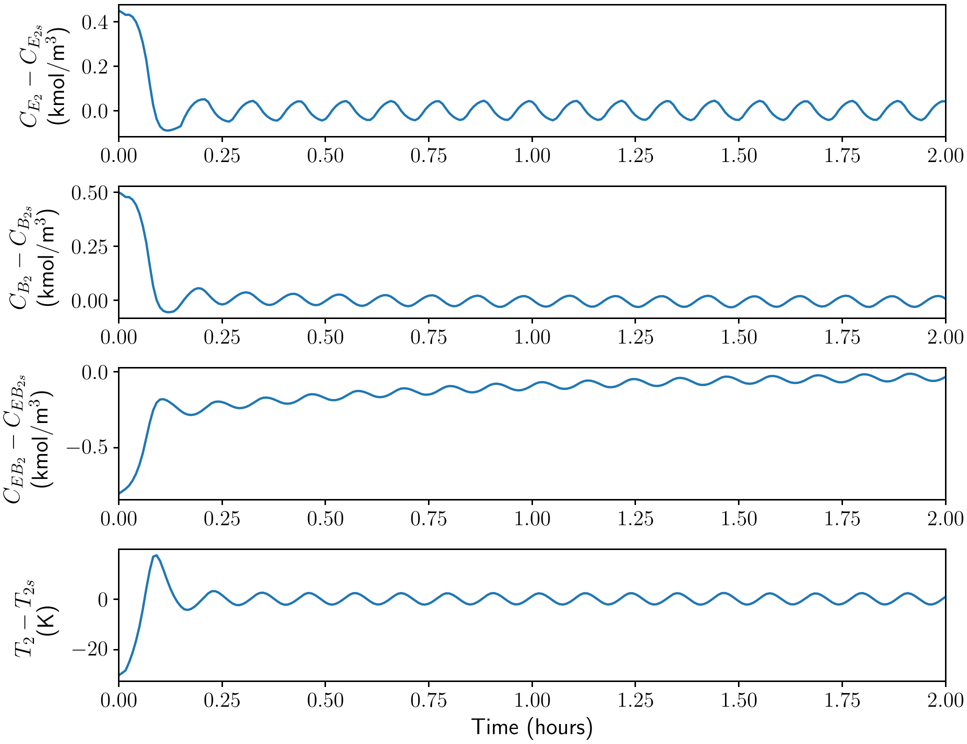

Fig. 4. State profiles of CSTR 2 under the encrypted decentralized LMPC for state delay $d_1 = 0.5$ min, and input delay $d_2 = 1$ min.

decentralized LMPC. While the latter stabilizes the states within Ω_ρ, it falls short of achieving convergence within the desired stability region after two hours of process time.

To measure the computational time for computing the control inputs in the decentralized MPC, we recorded the maximum time taken by the 2 MPCs at each sampling instance. On average, the decentralized controllers spent 2.49 s on control input computation at every sampling instance, whereas the centralized controller averaged 10.75 s. We ensured that the control input computation time remained below the 30-second sampling interval for all sampling times. These results demonstrate the computational efficiency of a decentralized MPC over a centralized MPC. Furthermore, the normalized sum of the control cost

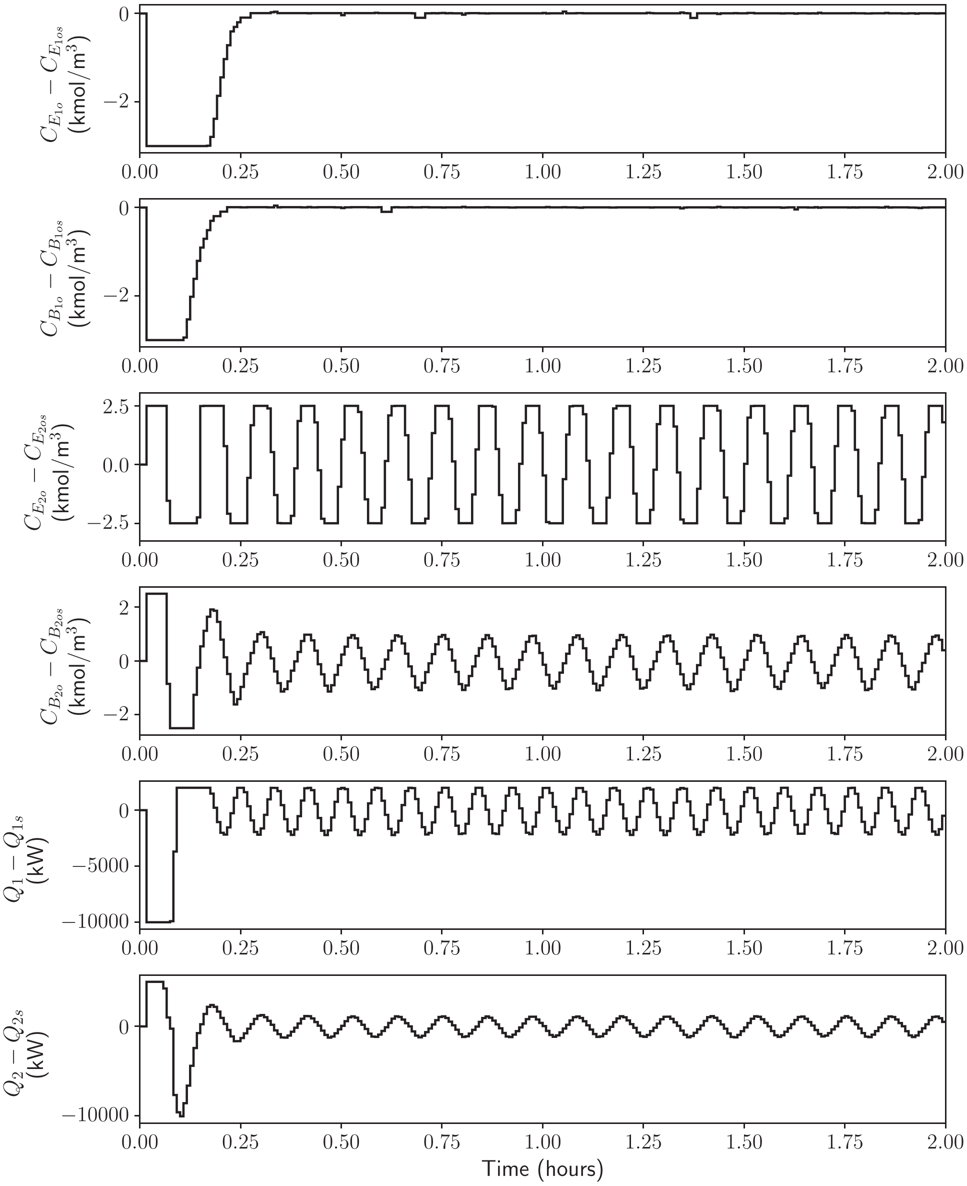

Fig. 5. Control input profiles under the encrypted decentralized LMPC for state delay $d_1 = 0.5$ min, and input delay $d_2 = 1$ min.

function for the centralized and decentralized MPCs without delays was recorded as 1 and 0.9798, respectively. The reason for a slightly better performance under the decentralized MPC can be attributed to the fact that the process network has a sequential flow sheet with 2 CSTRs in series, which makes the decentralized MPC a more suitable, well-conditioned choice than the centralized MPC with respect to the optimization problem solution. These results validate the effectiveness of the proposed decentralized LMPC framework in comparison to a centralized LMPC for this particular process network.

Remark 6. During the initial delay period, where control input information is not yet available, we assume steady-state values for the control inputs. This assumption results in a sharp increase that would not typically occur during continuous operation. To mitigate such abrupt changes in control inputs, one approach is to introduce a constraint on the maximum allowable change in applied control inputs between sampling instances. This constraint can help smooth the transition between steady-state values and actual control inputs initially, and also reduce sudden spikes or fluctuations in the system's behavior for the remainder of the operation.

Remark 7. The encrypted decentralized LMPC explored in this study involved encrypting and decrypting data as outlined in Fig. 1, which can lead to errors due to quantization. Suryavanshi et al. (2023) demonstrated quantization effects in the context of a first-principles-based MPC. Additionally, Kadakia et al. (2023) highlighted the potential for quantization-induced errors to exceed model mismatch errors when different models are employed in the MPC and in the controlled process. To minimize the quantization error, both works recommended using a higher quantization parameter d. With $d = 8$, both works reported almost identical closed-loop results with encryption compared to without encryption. Thus, we have used the quantization parameter, $d = 8$ for all simulations in this work.

Remark 8. In this work, we have assumed the same value of the input delay for all the control inputs applied to the nonlinear process. However, if the input delay values are different for certain control inputs, in the proposed encrypted decentralized control structure, the subsystems can be partitioned in a manner such that the control inputs manipulated by each subsystem have the same input delay values. Thus, the predictor of a particular subsystem would predict the states up to the

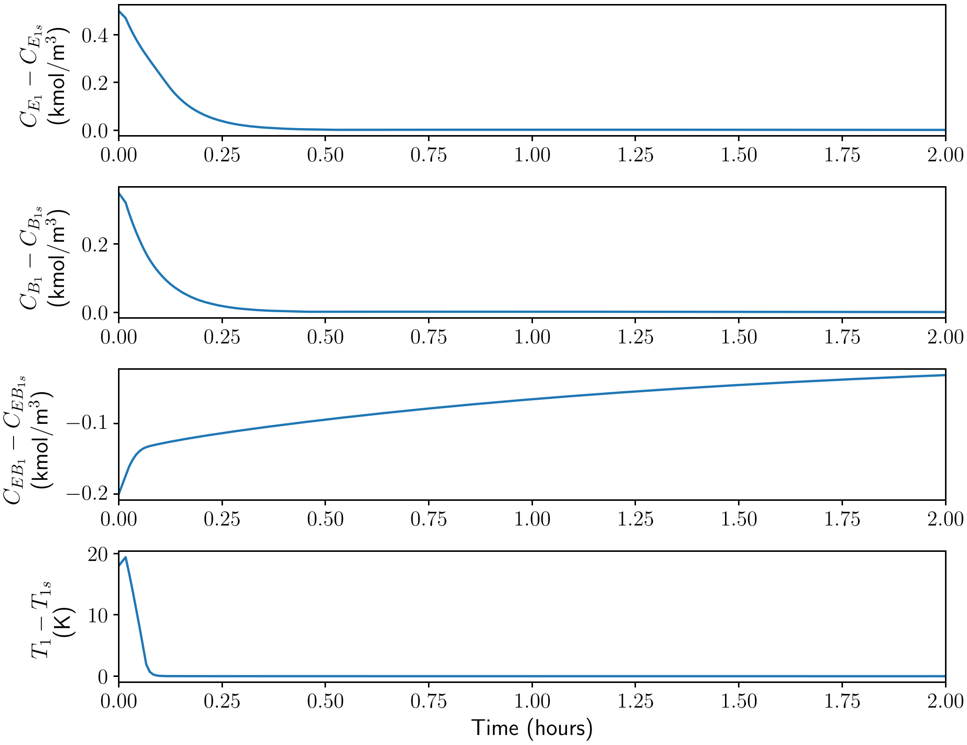

Fig. 6. State profiles of CSTR 1 under the encrypted decentralized LMPC with predictor feedback for state delay $d_1 = 0.5$ min, and input delay $d_2 = 1$ min.

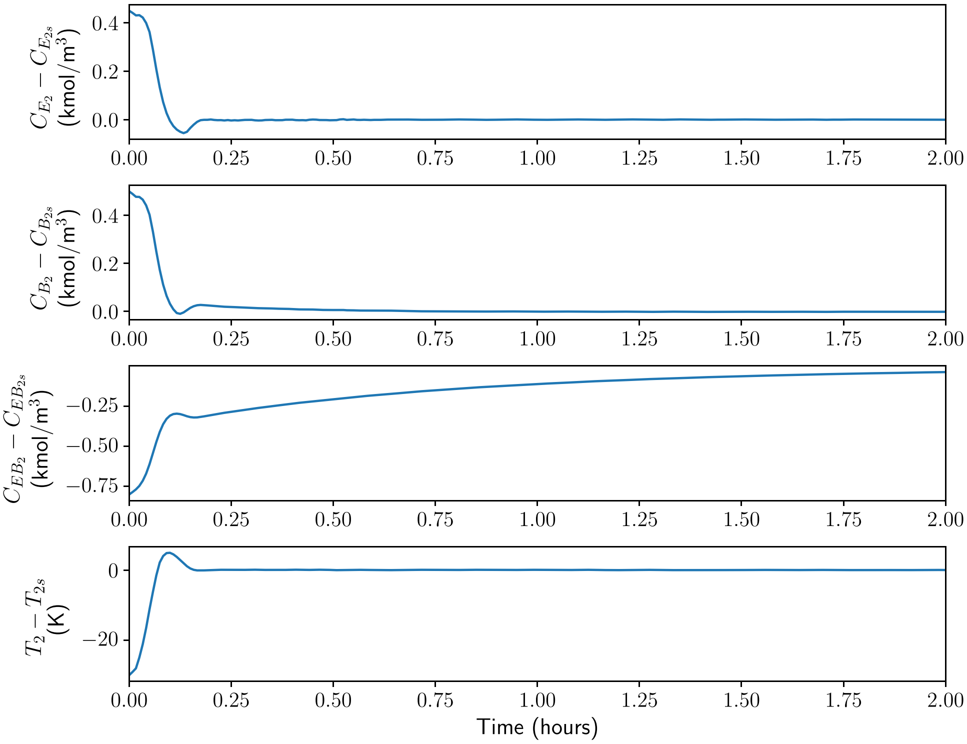

Fig. 7. State profiles of CSTR 2 under the encrypted decentralized LMPC with predictor feedback for state delay $d_1 = 0.5$ min, and input delay $d_2 = 1$ min.

corresponding input delay value of the control inputs manipulated by that subsystem.

Remark 9. Although the LMPC and predictor models used in this work are first-principles-based, data-based models employing artificial neural networks can also be used in the predictor and LMPC. Alnajdi et al. (2023) used machine-learning-based models for the predictor and LMPC while simulating a first-principles-based process with state and input delays, showcasing the effectiveness of the predictor in the presence of plant/model mismatch.

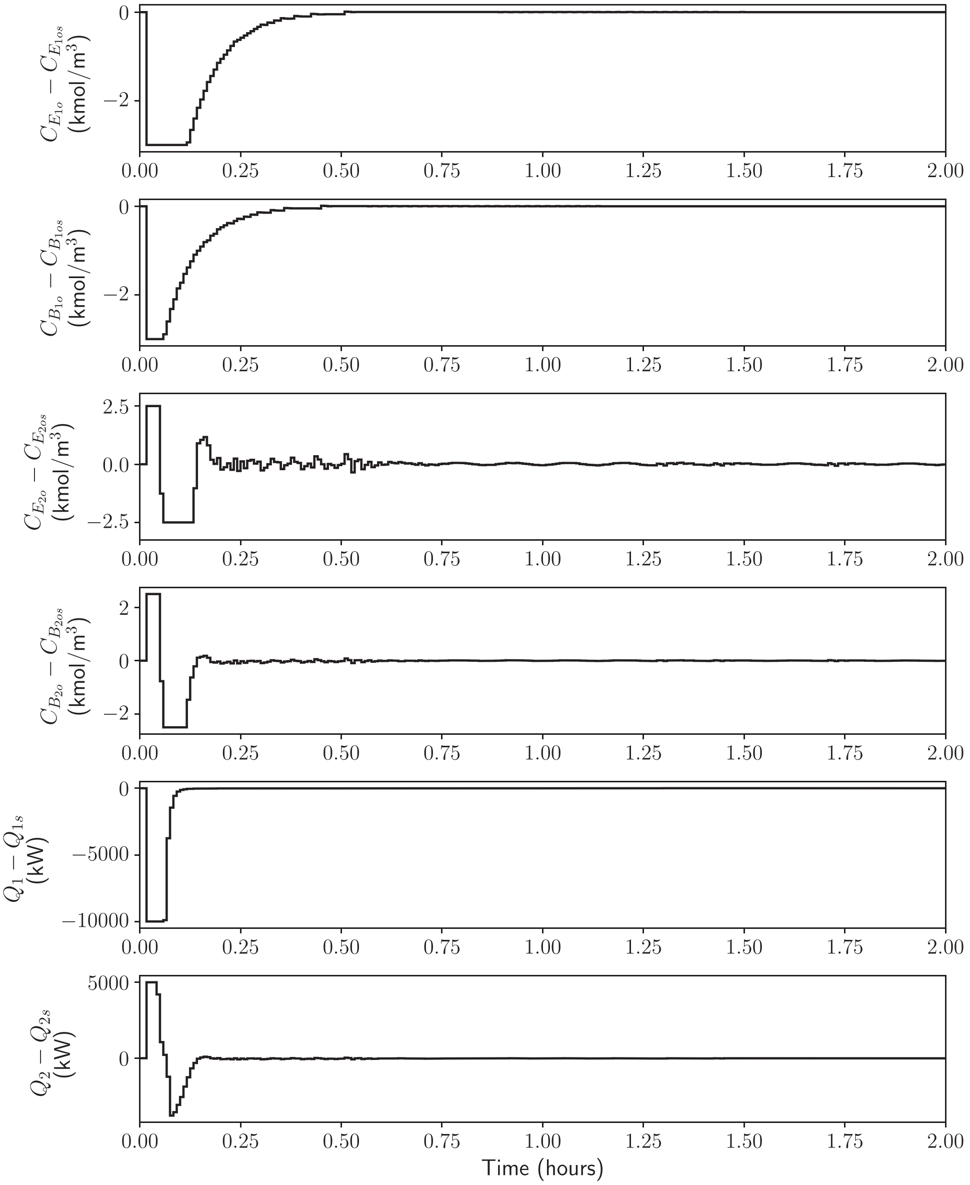

Fig. 8. Control input profiles under the encrypted decentralized LMPC with predictor feedback for state delay $d_1 = 0.5$ min, and input delay $d_2 = 1$ min.

5. Conclusion

In this study, we devised and applied an encrypted decentralized control architecture to a large-scale nonlinear chemical process network with input and state delays. A stability analysis of the encrypted decentralized MPC applied to a nonlinear system with state delays was conducted, yielding bounds on the errors due to quantization, state delays, and sample-and-hold implementation of the controller. Based on these bounds, the system can be stabilized within the desired stability region. We established guidelines to implement this control structure in any nonlinear process, such as selection of parameters l_1, l_2, and d for quantization, and the sampling time criterion. The encrypted decentralized LMPC employs a DDE model to account for state delays in the process. Closed-loop simulations are compared with and without the incorporation of a predictor into the LMPC design, where the predictor predicts the state values after the input delay period. A significant improvement in the closed-loop performance was observed with the integration of the predictor, as the states and inputs converged to their steady state values with negligible oscillations. Also, with the inclusion of the predictor, states converged within the desired stability region represented by the level set $\Omega_{\rho_{\min}}$. However, without the predictor, the states only stabilize within the larger level set Ω_ρ and with oscillations. Thus, by employing the encrypted decentralized LMPC with predictor feedback, we were able to reduce the computation time and complexity of the control problem, improve the closed-loop performance, and enhance the cybersecurity of the control system.

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.

Acknowledgement

Financial support from the National Science Foundation, CBET-2227241, is gratefully acknowledged.

References

Al-Abassi, A., Karimipour, H., Dehghantanha, A., Parizi, R.M., 2020. An ensemble deep learning-based cyber-attack detection in industrial control system. IEEE Access 8, 83965–83973.

Alnajdi, A., Suryavanshi, A., Alhajeri, M.S., Abdullah, F., Christofides, P.D., 2023. Machine learning-based predictive control of nonlinear time-delay systems: closed-loop stability and input delay compensation. Digit. Chem. Eng. 7, 100084.

Bakule, L., 2008. Decentralized control: an overview. Annu. Rev. Control 32, 87–98.

Conklin, W.A., 2016.IT vs. OT security: A time to consider a change in CIA to include resilienc, In: Proceedings of 49th Hawaii International Conference on System Sciences, Koloa, Hawaii.2642–2647.

Data61, C., 2013. Python paillier library.〈https://github.com/data61/python-paillier〉.

Darup, M.S., 2020. Encrypted MPC based on ADMM real-time iterations. IFAC-Pap. 53, 3508–3514.

Darup, M.S., Redder, A., Quevedo, D.E., 2018. Encrypted cloud-based MPC for linear systems with input constraints. IFAC-Pap. 51, 535–542.

Darup, M.S., Redder, A., Shames, I., Farokhi, F., Quevedo, D., 2017. Towards encrypted MPC for linear constrained systems. IEEE Control Syst. Lett. 2, 195–200.

Dutta, V., Choraś, M., Pawlicki, M., Kozik, R., 2020. A deep learning ensemble for network anomaly and cyber-attack detection. Sensors 20, 4583.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., Laplante, P., 2011. Dimensions of cyber-attacks: cultural, social, economic, and political. IEEE Technol. Soc. Mag. 30, 28–38.

Hale, J.K., Lunel, S.M.V., 1993. Introduction to functional differential equations. Springer, New York.

Kadakia, Y.A., Suryavanshi, A., Alnajdi, A., Abdullah, F., Christofides, P.D., 2023. Encrypted model predictive control of a nonlinear chemical process network. Processes 11, 2501.

Khan, R., Maynard, P., McLaughlin, K., Laverty, D., Sezer, S., 2016.Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid, in: Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research, Belfast, United Kingdom.1–11.

Narasimhan, S., El-Farra, N.H., Ellis, M.J., 2022. A control-switching approach for cyberattack detection in process systems with minimal false alarms. AIChE J. 68, e17875.

Narasimhan, S., El-Farra, N.H., Ellis, M.J., 2023. A reachable set-based scheme for the detection of false data injection cyberattacks on dynamic processes. Digit. Chem. Eng. 7, 100100.

Nieman, K., Messina, D., Wegener, M., Durand, H., 2023. Cybersecurity and dynamic operation in practice: equipment impacts and safety guarantees. J. Loss Prev. Process Ind. 81, 104898.

Paillier, P., 1999.Public-key cryptosystems based on composite degree residuosity classes, In: Proceedings of the International conference on the theory and applications of cryptographic techniques, Springer, Berlin, Heidelberg.223–238.

Paridari, K., O'Mahony, N., Mady, A.E.D., Chabukswar, R., Boubekeur, M., Sandberg, H., 2017. A framework for attack-resilient industrial control systems: attack detection and controller reconfiguration. Proc. IEEE 106, 113–128.

Smith, O.J., 1957. Closer control of loops with dead time. Chem. Eng. Prog. 53, 217–219.

Suryavanshi, A., Alnajdi, A., Alhajeri, M., Abdullah, F., Christofides, P.D., 2023. Encrypted model predictive control design for security to cyberattacks. AIChE J. 69, e18104.

Tsvetanov, T., Slaria, S., 2021. The effect of the colonial pipeline shutdown on gasoline prices. Econ. Lett. 209, 110122.

Wächter, A., Biegler, L.T., 2006. On the implementation of an interior-point filter line-search algorithm for large-scale nonlinear programming. Math. Program. 106, 25–57.

Wu, Z., Chen, S., Rincon, D., Christofides, P.D., 2020. Post cyber-attack state reconstruction for nonlinear processes using machine learning. Chem. Eng. Res. Des. 159, 248–261.