Robust and Resilient Distributed MPC for Cyber-Physical Systems Against DoS Attacks

Yufan Dai, *Graduate Student Member, IEEE*, Manyun Li, Kunwu Zhang, *Member, IEEE*, and Yang Shi, *Fellow, IEEE*

***Abstract*—In this article, considering the ubiquitously existing cyber attacks in cyber-physical systems (CPSs), we present a robust and resilient distributed model predictive control (MPC) strategy for CPSs with multi-agent architecture under denial-of-service (DoS) attacks to achieve the goal of cooperative regulation with all agents' states being regulated to their equilibrium. Each agent in the CPSs is subject to external disturbances, and the communication channels among agents might be affected by randomly occurring DoS attacks. To tackle these issues, firstly, a novel robustness constraint is designed to handle the uncertainties in the MPC algorithm. By adding this constraint, the state of the nominal system can be confined in a shrinking and tighter range compared to the classical MPC approach, thus resulting in enhanced robustness against uncertainties. Furthermore, a lengthened sequence transmission strategy is proposed to mitigate the effect of the lack of information in the communication channels induced by DoS attacks. At each time instant, the controller of each agent utilizes the predicted state information to compensate for the transmission block-out from one agent to another. Moreover, recursive feasibility for the control framework and the closed-loop stability for the overall system are guaranteed by theoretical analysis. Finally, simulation and comparison studies demonstrate the effectiveness of the proposed robust and resilient distributed MPC strategy.**

***Index Terms*—Cyber-physical systems, distributed MPC, DoS attacks, multi-agent systems, nonlinear systems.**

I. Introduction

NOWADAYS, cyber-physical systems (CPSs) gained increasing research attention in various areas because the seamless integration of cyber and physical domains has successfully stimulated many exciting applications in the era of Industry 4.0 [1]. These systems can be characterized as intelligent systems that comprise a combination of hardware, software, and computational and physical components, closely interacting to continuously sense and control the changing state of the real world in real-time [2]. CPSs are also characterized by being large-scale, distributed, and heterogeneous interconnected systems that span over various application domains [3]. Multi-agent CPS, consequently, is one of the major fields in CPSs, since it has a networked and distributed architecture for the purpose of collaboration among agents to solve a task [4], [5], which contributes to many areas, including spacecraft systems [6], multi-robot systems [7], modern highway transportation systems [8], etc.

However, great efficiency with the advent of the network in control systems also introduces high risks of cyber attacks, such as denial-of-service (DoS) attacks [9], [10], false data injection (FDI) attacks [11], replay attacks [12], etc. These attacks are sent purposely to jam the communication channels, steal the data, or tamper with the signal, causing severe security threats or even potential damage to the systems. Thus, the vulnerability toward cyber attacks is still a challenge and, thus, an emerging research issue in CPSs [13]. When these attacks are launched, the attackers are able to tamper or block the data transmitted from one component to another to prevent the overall system from achieving its control objectives. In this regard, the need for designing a control framework to mitigate the jeopardization caused by cyber attacks is of incremental urgency and paramount importance.

Model predictive control (MPC) offers a promising solution to solve the problem mentioned above. In general, MPC is often utilized due to its ability of handling the physical constraints while ensuring the optimal performance with respect to the preassigned indexes at the same time [14]. In addition to this, MPC also has the intrinsic advantage to tackle the attacks since at each sampling time instant, the controller generates not only the control input sequence including the current control input and the predicted control inputs but also the predicted state sequence, by performing the online optimization based on the plant model. Both predicted sequences can be deliberately utilized to play an instrumental role in proposing the resilient MPC strategy. Specifically, they can be effectively adopted to compensate for information loss caused by the DoS attacks or compare with the false data induced by deception attacks. Some resilient MPC strategies, dealing with cyber attacks, have recently been emerging and reported in the literature [13]. In [15], [16], the packet transmission strategy is applied to compensate for the lack of information caused by DoS attacks in the controller-to-actuator (C-A) channel for linear CPSs; a buffer is designed to store the predicted sequences. In [17], a resilient control strategy is proposed for nonlinear CPS and the event-triggered mechanism is employed to reduce the computational and communication

Manuscript received 22 February 2023; revised 22 April 2023; accepted 12 May 2023. Date of publication 6 June 2023; date of current version 27 June 2023. This work was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC). *(Corresponding author: Yang Shi.)*

The authors are with the Department of Mechanical Engineering, University of Victoria, Victoria, BC V8W 2Y2, Canada (e-mail: yufandai@uvic.ca; li.mnanyun@gmail.com; kunwu@uvic.ca; yshi@uvic.ca).

Digital Object Identifier 10.1109/TICPS.2023.3283229

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

load. In [18], a self-triggered resilient MPC framework is proposed to tackle the FDI attacks on the C-A channel in a CPS. In [19], a resilient control framework is designed for a CPS to detect and mitigate the effect induced by the replay attacks on the sensor-to-controller (S-C) channel. In [20], both DoS and FDI attacks are considered to interfere with the C-A channels in CPSs with limited energy. In spite of these attacks, the resilient MPC strategy proposed in this work is able to regulate the states while reducing the computational load by using the event-triggered mechanism. In summary, existing results show the effectiveness of the resilient MPC strategies to tackle cyber attacks, however, all the above-mentioned results only focus on the resilient MPC design for a single agent.

When it comes to a CPS involving multiple agents that are inter-connected via a communication network, the synthesis, and analysis of the resilient MPC strategies become more yet challenging, yet practically demanding. As explained in [21], in a multi-agent CPS, cyber attacks might be launched onto the local control loops of each involved agent, or onto the communication channels among agents. For example, in [22], a resilient distributed MPC strategy is proposed for the multi-agent system (MAS) in which each agent might suffer from FDI attacks that tamper with the state information transmitted in the S-C channels. In [23], the authors proposed a resilient distributed MPC scheme to detect and deal with replay attacks randomly launched to the S-C channel of the individual agent in the MAS. Furthermore, a distributed MPC strategy for the linear MASs is developed in [24] to tackle the DoS attacks that affect the S-C channel of each agent. The resilient distributed MPC strategy has also been studied to tackle the attacks on the C-A channel in each agent. In [25], a resilient distributed MPC algorithm is designed, considering the DoS attacks on the C-A channels of each agent for the linear MASs.

It is worthwhile mentioning that cyber attacks can be purposely launched on the communication channels among agents, thus adversely affecting information transmission among agents and aiming to destroy the safe system operation, but there exist very few results dedicated to this issue. In [26], a distributed MPC strategy is developed for a platoon problem, but it only considers DoS attacks that are launched on the channels between two nonconsecutive neighbor agents. In [27], the authors developed an event-triggered resilient distributed MPC method for the platoon problem of a linearized network-based vehicle system, in which a special case that DoS attacks directly target on the agent (the attacked agent cannot communicate with all its neighbors) is considered. However, the resilient distributed MPC framework against adversarial attacks randomly launching at all communication channels has not been adequately investigated. It is underscored that the following research questions need to be addressed: How to make full use of the “prediction” feature of MPC to efficiently compensate for the effect caused by DoS attacks? How to analyze the effect of DoS attacks on the theoretical properties of the resulting overall system? How to construct a resilient and robust distributed MPC strategy? The development and main results of this article will provide affirmative answers to the above questions.

In this article, a resilient and robust distributed MPC is proposed for multi-agent CPSs, specifically considering DoS attacks randomly occurring on the communication channels among agents. The main contributions of this work are three-fold:

1) Aiming at tackling the disturbances in the system, a new type of robustness constraint is constructed in the MPC optimization problem. Existing work about robustness constraint [28], [29], [30] mainly constructs the constraint only based on the terminal constraint, resulting in a small region of attraction. The proposed robustness constraint is designed based on both the state constraint and the terminal constraint, which can enlarge the region of attraction with comparable control performance;
2) A lengthened predicted state sequence scheme, depending on the attack duration, is proposed to facilitate the information transmission and efficient compensation for the lost information due to DoS attacks;
3) The rigorous theoretical analysis of the performance of the proposed robust and resilient distributed MPC are provided. Sufficient conditions on guaranteeing the recursive feasibility of the proposed method and stability of the closed-loop system are derived, respectively. A numerical example and comparison results are shown to illustrate the effectiveness of the resulting method.

The remainder of the article is organized as follows: Section II formulates the problem with some preliminary results. Section III describes the robust and resilient control framework. In Section IV, sufficient conditions for ensuring recursive feasibility and closed-loop stability are established, respectively. Numerical examples and comparison results are illustrated in Section V. Finally, the conclusion and future work are presented in Section VI.

I. Notations

The notations used in this article are fairly standard. The symbol $\mathbb{R}^n$ denotes the n-dimensional real space. The symbols $\mathbb{N}$ and $\mathbb{N}^+$ denote the set of all natural numbers and the set of all positive integers, respectively. Let $\mathbb{N}_{[a,\,b)}$ denote all the integers in the interval $[a,\,b], a < b$. Given a matrix P, $P \succ 0$ and $P \succeq 0$ denote that matrix P is positive definite and positive semidefinite, respectively. For a vector $x \in \mathbb{R}^{n\times 1}$, $\|x\|$ denotes the Euclidean norm and $\|x\|_P$ denotes the P weighted Euclidean norm as $\sqrt{x^{\mathrm{T}}Px}$, where the matrix $P \succ 0$. The difference between the two sets is defined as $A \setminus B \triangleq \{x|x \in A, x \notin B\}$. $\lambda_{\max}(P)$ and $\lambda_{\min}(P)$ denote the largest and the smallest eigenvalues of matrix P, respectively. $\lceil r \rceil$ rounds r to the nearest integer toward positive infinity.

II. Problem Formulation

A. System Description

The communication topology of a nonlinear multi-agent CPS consisting of M agents can be illustrated as a directed graph $\mathscr{G} \triangleq \{\mathscr{M}, \mathscr{E}\}$, where $\mathscr{M} = \{i\big|i = 1, 2, \ldots, M\}$ represents the set of all agents and $\mathscr{E} \subset \mathscr{M} \times \mathscr{M}$ is the collection of all the communication channels among agents. Furthermore, the neighbor set of agent i is denoted as $\mathscr{N}_i$. With such definition of the neighbor set, if agent i can receive information from its neighbors j, then $j \in \mathscr{N}_i$.

At the discrete-time sampling instant $k \in \mathbb{N}$, the model of agent $i \in \mathscr{M}$ is described as

$$x_i(k+1) = f_i(x_i(k), u_i(k)) + \omega_i(k), \tag{1}$$

where $f_i : \mathbb{R}^{n_x} \times \mathbb{R}^{n_u} \to \mathbb{R}^{n_x}$, $x_i(k) \in \mathbb{R}^{n_x}$ is the system state; $u_i(k) \in \mathbb{R}^{n_u}$ is the control input; $\omega_i(k) \in \mathbb{R}^{n_x}$ is the external disturbance. Here, the control input $u_i(k)$, the state $x_i(k)$, and the additive disturbance $\omega_i(k)$ are constrained by the following compact sets:

$$u_i(k) \in \mathbb{U}_i \subset \mathbb{R}^{n_u},\ x_i(k) \in \mathbb{X}_i \subset \mathbb{R}^{n_x},\ \omega_i(k) \in \mathbb{W}_i \subset \mathbb{R}^{n_x}, \tag{2}$$

with $\mathbb{U}_i$ and $\mathbb{X}_i$ containing the origin. In addition, $\rho \triangleq \sup_{\omega_i(k)\in\mathbb{W}_i} \|\omega_i(k)\|$ is defined as the upper bound of external disturbances.

For agent i, $i \in \mathscr{M}$, the nominal system of the system (1) is written as

$$\widehat{x}_i(k+1) = f_i(\widehat{x}_i(k), u_i(k)), \tag{3}$$

where $\widehat{x}_i(k)$ is the nominal state satisfying the state constraint $\widehat{x}_i(k) \in \mathbb{X}_i \subset \mathbb{R}^{n_x}$.

Assumption 1: For the system in (1), the following Lipschitz condition holds for all x_i, $z_i \in \mathbb{X}_i$ and $u_i \in \mathbb{U}_i$:

$$\|f_i(x_i, u_i) - f_i(z_i, u_i)\| \le L_{fi}\left(\|x_i - z_i\|\right), \tag{4}$$

where $L_{fi} > 0$ is the Lipschitz constant.

Assumption 2: For the nominal system (3), assume that:

- The point (0,0) is the equilibrium of the system, i.e., $f_i(0,0) = 0$, and $f_i : \mathbb{R}^{n_x} \times \mathbb{R}^{n_u} \to \mathbb{R}^{n_x}$ can be linearized at (0,0), and the linearized system is described as:

$$\widehat{x}_i(k+1) = A\widehat{x}_i(k) + Bu_i(k), \tag{5}$$

  where $A = \partial f_i/\partial x_i|_{(0,0)}$ and $B = \partial f_i/\partial u_i|_{(0,0)}$.
- For the linearized nominal system (5), there exists a state feedback control law $u_i(k) = K_i\widehat{x}_i(k)$ to make $A_{Ki} \triangleq A + BK_i$ stable.

Define the Lyapunov function $V_i(\widehat{x}_i(k)) \triangleq \|\widehat{x}_i(k)\|^2_{P_i}$ and the terminal set $\widehat{\Omega}_i(\epsilon_i) \triangleq \{x_i | x_i^{\mathrm{T}} P_i x_i \le \epsilon_i^2\}$, where $P_i \succ 0$ is the terminal penalty matrix.

Assumption 3: For the system in (3), suppose *Assumption 2* holds. Define $Q_i^* \triangleq Q_i + K_i^{\mathrm{T}} R_i K_i$, where $Q_i \succ 0$ and $R_i \succeq 0$ are two predesigned matrices with appropriate dimensions. There exist a constant $\epsilon_i > 0$, such that when $\widehat{x}_i \in \widehat{\Omega}_i(\epsilon_i)$.

- $V_i(\widehat{x}_i) = \widehat{x}_i^{\mathrm{T}} P_i \widehat{x}_i$ is chosen as the Lyapunov function to the system $\widehat{x}_i(k+1) = f_i(\widehat{x}_i, K_i\widehat{x}_i)$ and satisfies $V_i(\widehat{x}_i(k+1)) - V_i(\widehat{x}_i(k)) \le -\|\widehat{x}_i(k)\|^2_{Q_i^*}$;
- The candidate input $u_i = K_i\widehat{x}_i$ satisfies $K_i\widehat{x}_i \in \mathbb{U}_i$.

Note that the aforementioned assumptions are general and widely used in the related literature on MPC, e.g., [31], [32].

B. DoS Attacks

Due to the vulnerability of the communication channel, DoS attacks can interfere all the channels in CPS. Specifically, attacks in this work are set in an intermittent or random manner. When the DoS attack is in effect at any time instant, it will block the agent from broadcasting the predicted state sequence to its neigbors. Let $\mathscr{T}_{ij}^a \triangleq \{k_{ij,\ell}^a\}$ and $\mathscr{D}_{ij}^a \triangleq \{d_{ij,\ell}^a\}$ denote all the launching time instants and their corresponding duration of the DoS attacks on the channel from agent i to agent j, respectively. Here, ℓ denotes the ℓth launching. We define

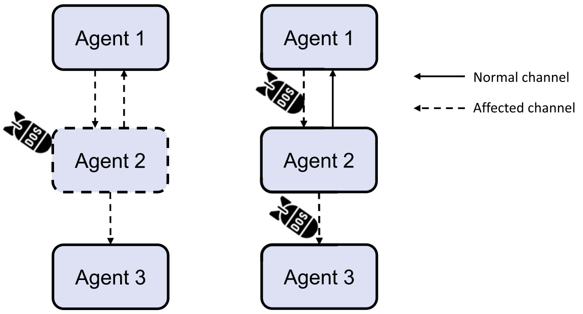


Fig. 1. DoS attacks occuring on agents (left) and communication channels among agents (right).

$$\Xi_{ij}(k_0, k_1) \triangleq \bigcup_{\ell\in\mathbb{N}} \mathbb{N}_{[k_{ij,\ell}^a,\, k_{ij,\ell}^a + d_{ij,\ell}^a)} \tag{6a}$$

$$\Theta_{ij}(k_0, k_1) \triangleq \mathbb{N}_{(k_0,\, k_1)} \setminus \Xi_{ij}(0,\, \infty) \tag{6b}$$

to represent the total activation time periods of DoS attacks, and the overall successful transmission time periods from i to j in the time interval $[k_0,\, k_1]$, respectively. The launching time instants and their corresponding duration satisfy $k_{ij,\ell}^a > k_0$, $k_{ij,\ell}^a + d_{ij,\ell}^a \le k_1$, where $k_0 \in \mathbb{N}$, $k_1 \in \mathbb{N}^+$, and $k_1 > k_0$.

Consequently, the effect of DoS attacks on the information transmission from i to j can be described as

$$\Phi_{ij,\Xi}(k) = \begin{cases} 1, & k \in \Xi_{ij}(k_0,\, k_1) \\ 0, & k \in \Theta_{ij}(k_0,\, k_1) \end{cases}, \tag{7}$$

where $\Phi_{ij,\Xi} = 1$ represents that the information transmission from i to j is blocked, and $\Phi_{ij,\Xi} = 0$ indicates a successful transmission. We recall the following assumption from [33] to characterize DoS attacks within finite time horizon.

Assumption 4: With the DoS attacks activation time being set as (6a), there exist constants $\alpha \ge 0$ and $\gamma \in (0, 1)$ such that for all $k_0 \ge 0$ and $k_1 \ge k_0$,

$$|\Xi_{ij}(k_0, k_1)| = \sum_{k=k_0}^{k_1} \Phi_{ij,\Xi}(k) \le \alpha + \gamma(k_1 - k_0), \tag{8}$$

where $|\Xi_{ij}(k_0, k_1)|$ represents all the activation time instants of DoS attacks between the time interval $[k_0,\, k_1]$.

Remark 1: Note that γ in (8) is defined as $\lim_{k_1\to\infty} \frac{|\Xi_{ij}(k_0,k_1)|}{k_1-k_0}$, which depicts the ratio of the total attack duration in considered time intervals. As a result, the upper bound of the duration of DoS attacks can be derived as $N_a \triangleq \lceil \alpha/(1-\gamma) \rceil$.

Remark 2: Different from the attacks that directly launch on the agents [27], we consider attacks on the arbitrary communication channels among agents. In general, attacks on the agents

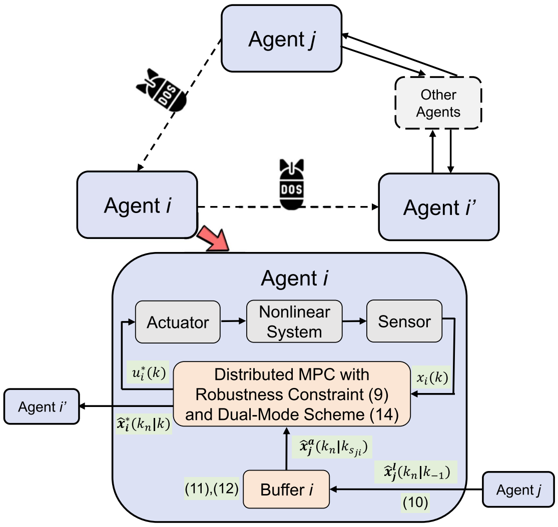

Agent j
Other Agents
DOS
DOS
Agent i
Agent i'
Agent i
Actuator
Nonlinear System
Sensor
$u_i^*(k)$
Distributed MPC with Robustness Constraint (9) and Dual-Mode Scheme (14)
$x_i(k)$
Agent i'
$\widehat{\boldsymbol{x}}_i^*(k_n|k)$
$\widehat{\boldsymbol{x}}_j^a(k_n|k_{s_{ji}})$
$\widehat{\boldsymbol{x}}_j^l(k_n|k_{-1})$
(11),(12)
Buffer i
Agent j
(10)

Fig. 2. Control framework of an multi-agent CPS at time instant k (focusing on Agent i).

block the information receiving and broadcasting channels simultaneously, which consequently can be seen as a special case of the problem formulated in our article. An illustrative example with three agents is given in the following for the explanation. For the left figure in Fig. 1 , based on the attack policy in [27], assume that agent 2 is attacked. Then it cannot receive information from agent 1, and cannot broadcast information to agent 1 and agent 3. This situation can be equivalently represented by the proposed formulation, in which all three communication channels are suffering DoS attacks, as shown in the right figure in Fig. 1. As a result, the attack policy in [27] can be considered as a special case of the proposed formulation.

C. Control Objectives

Consider a multi-agent CPS consisting of a group of agents whose model can be described in (1) and their connections are characterized as a directed graph. In this work, we aim to develop a robust and resilient distributed MPC strategy such that even under unknown disturbances and DoS attacks on the channels among agents, the states of all agents can be steered to a small region around the equilibrium in a cooperative manner.

III. Robust and Resilient Distributed MPC Against DoS Attacks

In this section, a robust and resilient distributed MPC strategy is proposed, as illustrated in Fig. 2. Firstly, the distributed MPC algorithm is introduced. By imposing a new robustness constraint to the MPC optimization problem, the effect of external disturbances is predicted to be confined within the tightened state constraint. Thus, the robustness of the MPC is enhanced. Furthermore, based on the optimal control sequence and state sequence from the MPC algorithm, a lengthened sequence transmission strategy is proposed to mitigate the effect caused by DoS attacks. Finally, a dual-mode scheme is proposed to reduce the unnecessary computational burden.

A. Distributed MPC With Robustness Constraint

To handle the external disturbances, we design the robustness constraint for the optimization problem of each agent. The robustness constraint is developed to shrink the state of the nominal system step by step in a predesigned manner to counter the effect caused by external disturbances. Specifically, the robustness constraint in this work is designed based on both state constraint and terminal constraint for the purpose of enlarging the region of attraction compared to [30]. Having added this constraint, we formulate the optimization problem $\mathscr{P}_i$ as:

$$\min_{\boldsymbol{u}_i(k_n|k)} \quad \left\{J_i\left(\widehat{x}_i(k_n|k), u_i(k_n|k), \widehat{x}^a_{-i}(k_n|k)\right)\right\}$$

$$\text{s.t.} \quad \widehat{x}_i(k|k) = x_i(k), \tag{9a}$$

$$\widehat{x}_i(k_{n+1}|k) = f_i\left(\widehat{x}_i(k_n|k), u_i(k_n|k)\right), \tag{9b}$$

$$u_i(k_n|k) \in \mathbb{U}_i, \tag{9c}$$

$$\|\widehat{x}_i(k_n|k)\| \le \left(1 - \frac{n}{N_p}\zeta_i\right)\mathscr{c}_i, \tag{9d}$$

$$\|\widehat{x}_i(k_{N_p}|k)\|_{P_i} \le \xi_i \epsilon_i, \quad n = 0, 1, \ldots, N_p - 1, \tag{9e}$$

where k_n denotes $k+n$, k_{N_p} denotes $k+N_p$, in which N_p is the prediction horizon. $\widehat{\boldsymbol{x}}_i(k_n|k)$ is defined as the state sequence of predicted nominal system state, which is generated through (9b) with the control input sequence $\boldsymbol{u}_i(k_n|k)$. $\widehat{x}^a_{-i}(k_n|k)$ is the collection of the assumed state of agent i's neighbors. (9c) is the input constraint. (9d) and (9e) are the robustness constraint, where ζ_i, ξ_i are scaling parameters for the tightened state constraint and terminal constraint, respectively. In addition, the positive constant $\mathscr{c}_i = \arg\max_{\mathscr{c}_i}\{\mathscr{c}_i \in \mathbb{R} : \mathbb{B}_i(\mathscr{c}_i) \subseteq \mathbb{X}_i\}$, where $\mathbb{B}_i(\mathscr{c}_i) \triangleq \{\widehat{x}_i | \|\widehat{x}_i\| \le \mathscr{c}_i\}$. By solving the optimization problem at time instant k, we can obtain the optimal input and state sequences as $\boldsymbol{u}_i^*(k_n|k) \triangleq \{u_i^*(k|k), u_i^*(k_1|k), \ldots u_i^*(k_{N_p-1}|k)\}$ and $\widehat{\boldsymbol{x}}_i^*(k_n|k) \triangleq \{\widehat{x}_i^*(k|k), \widehat{x}_i^*(k_1|k), \ldots \widehat{x}_i^*(k_{N_p}|k)\}$, respectively.

Here, the objective function is defined as $J_i(\widehat{x}_i(k), u_i(k), \widehat{x}^a_{-i}(k)) = \sum_{n=0}^{N_p-1}\{\|\widehat{x}_i(k_n|k)\|^2_{Q_i} + \|u_i(k_n|k)\|^2_{R_i} + \sum_{j\in\mathcal{N}_i} \|\widehat{x}_i(k_n|k) - \widehat{x}^a_j(k_n|k)\|^2_{Q_{ji}}\} + \|\widehat{x}_i(k_{N_p}|k)\|^2_{P_i}$, where $\widehat{x}^a_j(k_n|k)$ is the assumed state sent from agent j, $j \in \mathcal{N}_i$, which will be discussed in III-B. $Q_i \succ 0$ and $R_i \succeq 0$ are the weighting matrices, and $Q_{ji} \succ 0$ is the cooperation matrix.

B. Lengthened Sequence Transmission Strategy

To tackle the randomly occurring DoS attacks on the communication channels among agents, we design a lengthened sequence transmission strategy. Considering three agents in a multi-agent system, i, j, and i'. Agent i needs to receive information from agent j and agent i' needs to receive information from agent i at each time instant. Considering the attacks on the j to i channel at the time instant k, agent j generates lengthened state and control input sequences using the following strategy:

$$\boldsymbol{u}_j^l(k_n|k) = \begin{cases} u_j^*(k_n|k) & \text{if } n \in \mathbb{N}_{[0,N_p-1]}, \\ K_i \widehat{x}_i^l(k_n|k) & \text{if } n \in \mathbb{N}_{[N_p, N_p+N_a-1]} \end{cases}$$

$$\widehat{x}_j^l(k_{n+1}|k) = f_j\left(\widehat{x}_j^l(k_n|k), u_j^l(k_n|k)\right), \ n \in \mathbb{N}_{[0,N_p+N_a-1]} \tag{10}$$

where $\boldsymbol{u}_j^l(k_n|k)$ and $\widehat{\boldsymbol{x}}_j^l(k_n|k)$ are the lengthened control input and state sequences, N_a is the upper of the duration of the DoS attacks defined in *Remark* 1, and $\widehat{x}_j^l(k|k) = x_j(k)$.

The lengthened sequence to be sent from agent j to agent i depends on whether the channel from j to i is attacked, which is explained in the following. Before showing details, we firstly define $k_{s_{ji}}$ as the latest successful transmission instant from agent j to agent i. Then the following two cases are considered:

- When the communication channel from j to i is not attacked at the time instant $k-1$, agent i can receive the information generated from agent j, and save this sequence in the buffer. In this case, at time instant k, the MPC controller in agent i directly utilizes the state sequence at the time instant $k-1$ with
$$\widehat{\boldsymbol{x}}_j^a(k_n|k) = \widehat{\boldsymbol{x}}_j^l(k_n|k_{-1}), \ n \in \mathbb{N}_{[0,N_p-1]}. \tag{11}$$
After employing the sequence in the optimization problem $\mathscr{P}_i$, update $k_{s_{ji}} = k-1$. Having done this, the optimization problem can be solved to generate two sequences $\boldsymbol{u}_i^*(k_n|k)$ and $\widehat{\boldsymbol{x}}_i^*(k_n|k)$. Finally, agent i lengthens the state and control input sequences with the same step as (10), and sends the lengthened state sequence to agent i'.
- When the communication channel from j to i is being attacked at the time instant $k-1$, agent i cannot receive the information generated from agent j. In this case, select part of the state sequence saved at the time instant $k_{s_{ji}}$ in the buffer with
$$\widehat{\boldsymbol{x}}_j^a(k_n|k) = \widehat{\boldsymbol{x}}_j^l(k_n|k_{s_{ji}}), \ n \in \mathbb{N}_{[0,N_p-1]}. \tag{12}$$
Then, the MPC controller adopts $\widehat{x}_j^a(k_n|k)$ as the neighbor's state sequence and generates two optimal sequences $\boldsymbol{u}_{\boldsymbol{i}}^*(k_n|k)$ and $\widehat{\boldsymbol{x}}_{\boldsymbol{i}}^*(k_n|k)$. Finally, similar to the first case, after lengthening the state and control input sequences by following (10), agent i broadcasts the lengthened state sequence to agent i'.

Remark 3: Note that there is a special case when $k=0$, the strategy above is not applicable since the sequence $\widehat{\boldsymbol{x}}_i^a(k_n|k)$, $i \in \mathscr{M}$, does not exist. In this regard, we set $\widehat{\boldsymbol{x}}_i^a(n|0)$ to be an all-zeros sequence.

Remark 4: Under the lengthened sequence transmission strategy, the successful data transmission time instant $k_{s_{ji}}$ is updated only when the communication channel is not attacked at that time instant. As a result, at time instant k, each agent in the CPS can determine whether DoS attacks have occurred on their information-receiving channels by comparing the values of $k_{s_{ji}}$ and $k-1$. If $k_{s_{ji}}$ does not match the last time instant, it indicates that DoS attacks have affected the communication channel.

C. Dual-Mode Control Framework

Dual-mode control has been widely applied in a variety of the MPC schemes; see, e.g., [30], [34], [35]. It is known that it can help reduce the computational burden, because when the states of all the agents enter the terminal region at the time instant k_o:

$$\|\widehat{x}_i(k_o|k_o)\|_{P_i}^2 \leq {\epsilon_i}^2, \tag{13}$$

the control scheme is changed to the state-feedback control law

$$u_i(k_o) = K_i x_i(k_o), \tag{14}$$

rather than solving Problem $\mathscr{P}_i$. Furthermore, when the channel is suffering from DoS attacks, the dual-mode control can help enhance the resilience against attacks, since the state-feedback control law does not require the information from neighbor agents. In addition, we assume that there exists a detection mechanism for each agent, such that each agent can know whether the states of other agents enter the terminal region. As a result, the attacks launching on the communication channels will not affect the control input generation.

Based on the previous discussions, the proposed robust and resilient distributed MPC strategy will be implemented in a dual-mode control manner, which is summarized in Algorithm 1.

IV. Theoretical Analysis

This section shows the proof for the recursive feasibility of the formulated optimization problem and the closed-loop stability of the multi-agent CPS by applying the proposed resilient and robust distributed MPC approach.

For agent i, $i \in \mathscr{M}$, construct a candidate control sequence at the time instant $k+1$

$$\widetilde{\boldsymbol{u}}_i(k_n|k_1) \triangleq \left\{\widetilde{u}_i(k_1|k_1), \widetilde{u}_i(k_2|k_1), \ldots, \widetilde{u}_i(k_{N_p}|k_1)\right\},$$

and its corresponding state sequence

$$\widetilde{\boldsymbol{x}}_i(k_n|k_1) \triangleq \left\{\widetilde{x}_i(k_1|k_1), \widetilde{x}_i(k_2|k_1), \ldots, \widetilde{x}_i(k_{N_p+1}|k_1)\right\},$$

where the candidate control sequence $\widetilde{\boldsymbol{u}}_i(k_{n+1}|k_1)$, $n \in \mathbb{N}_{[0,\,N_p-1]}$ can be represented as

$$\widetilde{\boldsymbol{u}}_i(k_{n+1}|k_1) = \begin{cases} u_i^*(k_{n+1}|k) & \text{if } \ n \in \mathbb{N}_{[0,N_p-2]} \\ K_i \widehat{x}_i^*(k_{N_p}|k) & \text{if } \ n = N_p - 1 \end{cases}, \tag{15}$$

and the predicted state sequence $\widetilde{\boldsymbol{x}}_i(k_{n+1}|k_1)$ are constructed according to the nominal system dynamics

$$\widetilde{x}_i(k_{n+1}|k_1) = f_i\left(\widetilde{x}_i(k_n|k_1), \widetilde{u}_i(k_n|k_1)\right), \ n \in \mathbb{N}_{[0,N_p-1]}. \tag{16}$$

For the rest of this section, we will prove that the candidate input sequence and its corresponding predicted state sequence can be the feasible solution of optimization problem $\mathscr{P}_i$ under certain conditions, and the multi-agent CPS is stable based on the feasibility analysis.

A. Recursive Feasibility

In this subsection, we conduct the feasibility analysis of the formulated optimization problem and derive the sufficient conditions of ensuring the recursive feasibility. Before proceeding, we present the following assumption and lemma that will be used to establish the main results.

Assumption 5: Assume that there exists an initially feasible region $\mathbb{X}_N \subseteq \mathbb{X}_i$, such that for all the initial state $x_0 \in \mathbb{X}_N$, the

Algorithm 1: Robust and Resilient Distributed MPC Algorithm.

```
Require: For agent $i$, $i \in \mathscr{M}$, the weighting matrices $Q_i$, $Q_{ji}$, $R_i$; the state-feedback control gain $K_i$; the terminal penalty matrix $P_i$; the prediction horizon $N_p$; the terminal set level $\epsilon_i$; scaling parameters $\xi_i$ and $\zeta_i$; the initial state $x_i(0)$; the upper bound of the duration of DoS attacks $N_a$. Set $k = 0$, and $k_{s_{ji}} = 0$.
while the control action is not stopped do
  For all agents, sample the system states.
  if (13) is not satisfied for all the agents then
    for agent $i$, $i \in \mathscr{M}$ do
      if the communication channels from $j$ to $i$, $j \in \mathscr{N}_i$, is not being attacked then
        Receive state sequence $\widehat{\boldsymbol{x}}^l_j(k_n|k_{-1})$ from its neighbors $j$.
        Save the state sequence $\widehat{\boldsymbol{x}}^l_j(k_n|k_{-1})$ in the buffer and update $k_{s_{ji}} = k - 1$.
      else
        Adopt the sequence $\widehat{\boldsymbol{x}}^l_j(k_n|k_{s_{ji}})$ saved in the buffer.
      end if
    end for
    Construct the state sequence by following (11), (12), and send it to the MPC controller.
    Solve the optimization problem $\mathscr{P}_i$ to generate the sequence $\boldsymbol{u}^*_i(k_n|k)$ and $\widehat{\boldsymbol{x}}^*_i(k_n|k)$.
    Apply $u_i(k) = u^*_i(k|k)$ to agent $i$.
    Construct the lengthened state and control input sequences by applying (10), and then broadcast the state sequence to its neighbors.
  else
    for agent $i$, $i \in \mathscr{M}$ do
      Construct the control input by applying (14).
    end for
  end if
  $k = k + 1$;
end while
```

optimization problem in (9) admits a feasible solution when its initial value is set as x_0.

To guarantee recursive feasibility, essentially it suffices to prove that the predicted state sequences generated at the time instant $k+1$ under the candidate control input sequence is feasible. More specifically, it does need the following three requirements to be fulfilled.

(R1) The predicted state at the time instant $k + N_p$ satisfies the terminal constraint:

$$\|\widetilde{x}_i(k_{N_p}|k_1)\|_{P_i} \leq \epsilon_i. \tag{17}$$

(R2) The predicted state at the time instant $k + N_p + 1$ satisfies the tightened terminal constraint:

$$\|\widetilde{x}_i(k_{N_p+1}|k_1)\|_{P_i} \leq \xi_i\epsilon_i. \tag{18}$$

(R3) The predicted state satisfies the tightened state constraint:

$$\|\widetilde{x}_i(k_{n+1}|k_1)\| \leq \left(1 - \frac{n}{N_p}\zeta_i\right)\epsilon_i. \tag{19}$$

Lemma 1: For agent $i \in \mathscr{M}$, with the system dynamics in (1), suppose *Assumptions 1* and *2* hold, and optimization problem $\mathscr{P}_i$ has a feasible solution at the time instant k, then $\|\widetilde{x}_i(k_n|k_1) - \widehat{x}^*_i(k_n|k)\| \leq {L_{fi}}^{n-1}\rho$, $n \in \mathbb{N}_{[1,N_p]}$.

Proof: Recall that at the time instant k, the optimal input sequence is denoted as $\boldsymbol{u}^*_i(k_n|k), n \in \mathbb{N}_{[0,\,N_p-1]}$ and the optimal state sequence is denoted as $\widehat{\boldsymbol{x}}^*_i(k)$, $n \in \mathbb{N}_{[0,\,N_p]}$. The upper bound of the difference between the optimal state and the actual state can be derived as:

$$\begin{aligned} &\|\widehat{x}^*_i(k_n|k_{n-1}) - x_i(k_n)\| \\ &= \|f_i\left(\widehat{x}^*_i(k_{n-1}|k_{n-1}), u_i(k_{n-1})\right) \\ &\quad - f_i\left((x_i(k_{n-1}), u_i(k_{n-1})) - w_i(k_{n-1})\right\| \\ &\leq \rho, \end{aligned} \tag{20}$$

where $n \in \mathbb{N}_{[1,N_p]}$.

Similarly, the difference between the nominal state and the optimal sequence can be derived as

$$\begin{aligned} &\|\widetilde{x}_i(k_n|k_1) - \widehat{x}^*_i(k_n|k)\| \\ &= \|f_i\left(\widetilde{x}_i(k_{n-1}|k_1), \widetilde{u}_i(k_{n-1}|k_1)\right) \\ &\quad - f_i\left(\widehat{x}^*_i(k_{n-1}|k), u^*_i(k_{n-1}|k)\right)\| \\ &\overset{(4)}{\leq} L_{fi}\|\widetilde{x}_i(k_{n-1}|k_1) - \widehat{x}^*_i(k_{n-1}|k)\| \\ &\leq {L_{fi}}^{n-1}\|\widetilde{x}_i(k_1|k_1) - \widehat{x}^*_i(k_1|k)\| \\ &= {L_{fi}}^{n-1}\|x_i(k_1) - \widehat{x}^*_i(k_1|k)\| \\ &\overset{(20)}{\leq} {L_{fi}}^{n-1}\rho, \end{aligned} \tag{21}$$

where $n \in \mathbb{N}_{[1,N_p]}$. ■

After deriving the difference between the nominal state and the optimal state at the same predicted time instant, we can obtain the following theorem to prove the recursive feasibility of the optimization problem $\mathscr{P}_i$.

Theorem 1: For agent $i \in \mathscr{M}$, suppose *Assumptions 1–5* hold, and the optimization problem $\mathscr{P}_i$ is feasible at the time instant k, Algorithm 1 is also feasible if the following conditions are satisfied:

$$\frac{\lambda_{\max}\left(P_i^{\frac{1}{2}}\right)}{\lambda_{\max}\left(P_i^{\frac{1}{2}}\right) + \lambda_{\min}\left(Q_i^{*\frac{1}{2}}\right)} \leq \xi_i \leq 1 - \frac{\rho\lambda_{\max}\left(P_i^{\frac{1}{2}}\right){L_{fi}}^{N_p-1}}{\epsilon_i} \tag{22a}$$

$$\zeta_i \geq \frac{N_p\rho {L_{fi}}^{N_p-1}}{\epsilon_i} \tag{22b}$$

where ξ_i and ζ_i are positive constants for agent $i \in \mathscr{M}$.

Proof: To complete the proof, we need to show that the candidate input sequence (15) and the corresponding predicted state sequence (16) satisfy the input constraint and conditions (R1)–(R3) when ξ_i and ζ_i satisfy the conditions above, which is explained in the following.

Before showing the details, we firstly demonstrate that the input constraint is satisfied. As shown in (15), the candidate input sequence $\widetilde{\boldsymbol{u}}_i(k_{n+1}|k_1)$ is constructed based on the optimal control input sequence $\boldsymbol{u}_i^*(k_n|k)$ and the feedback control law $K_i\widehat{x}_i^*(k_{N_p}|k)$. According to *Assumption 3*, the candidate input sequence always satisfies the input constraint.

(R1) At the time instant $k+1$, we need to prove that (17) is satisfied. By applying (21), one has

$$\|\widetilde{x}_i(k_{N_p}|k_1) - \widehat{x}_i^*(k_{N_p}|k)\|_{P_i} \leq \lambda_{\max}\left(P_i^{\frac{1}{2}}\right) {L_f}_i^{N_p-1}\rho. \quad (23)$$

By recalling the tightened terminal constraint at time instant k, $\|\widehat{x}_i^*(k_{N_p}|k)\|_{P_i} \leq \xi_i\epsilon_i$, and applying the triangle inequality, we can derive

$$\begin{aligned}&\|\widetilde{x}_i(k_{N_p}|k_1) - \widehat{x}_i^*(k_{N_p}|k)\|_{P_i} + \|\widehat{x}_i^*(k_{N_p}|k)\|_{P_i}\\ &\overset{(23)}{\leq} \lambda_{\max}\left(P_i^{\frac{1}{2}}\right) {L_f}_i^{N_p-1}\rho + \xi_i\epsilon_i. \quad (24)\end{aligned}$$

Since ξ_i satisfies (22a), it suffices to impose that

$$\lambda_{\max}\left(P_i^{\frac{1}{2}}\right) {L_f}_i^{N_p-1}\rho + \xi_i\epsilon_i \leq \epsilon_i.$$

Then it can be derived that (17) is satisfied.

(R2) We also need to ensure that (18) holds at the time instant $k+1$. Recalling the control input sequence constructed as (15), according to *Assumption 3*, we have:

$$\|\widetilde{x}_i(k_{N_p+1}|k_1)\|_{P_i} \leq \|\widetilde{x}_i(k_{N_p}|k_1)\|_{P_i} - \|\widetilde{x}_i(k_{N_p}|k_1)\|_{Q_i^*}.$$

With (22a) being met, the following inequality holds:

$$\max\left\{\|\widetilde{x}_i(k_{N_p}|k_1)\|_{P_i} - \|\widetilde{x}_i(k_{N_p}|k_1)\|_{Q_i^*}\right\} \leq \xi_i\epsilon_i,$$

which is the equivalent requirement of (18).

(R3) Finally, at the time instant $k+1$, we need to prove that (19) is satisfied. By applying (21), it can be obtained that

$$\|\widetilde{x}_i(k_n|k_1)\| \leq \|\widehat{x}_i^*(k_n|k)\| + {L_f}_i^{n-1}\rho,$$

where $n \in \mathbb{N}_{[1,N_p]}$. Due to the fact that ζ_i satisfies (22b), the following inequality is held:

$$\|\widetilde{x}_i(k_n|k_1)\| \leq \|\widehat{x}_i^*(k_n|k)\| + {L_f}_i^{n-1}\rho \leq \left(1 - \frac{n-1}{N_p}\zeta_i\right)\mathscr{c}_i.$$

Thus, the requirement (R3) is met.

In summary, according to Theorem 1, if the given conditions are satisfied, Algorithm 1 is recursively feasible. ■

B. Stability Analysis

As discussed in Theorem 1, the recursive feasibility of the formulated optimization problem can be guaranteed if a set of conditions can be satisfied. In this subsection, we concentrate on the closed-loop stability analysis of the multi-agent CPS by applying the proposed resilient and robust MPC strategy as illustrated in Algorithm 1.

Theorem 2: For the multi-agent CPS (1) using Algorithm 1 with *Assumptions 1–5* held. Given a constant β_i with $\frac{\lambda_{\max}\left(P_i^{\frac{1}{2}}\right)}{\lambda_{\max}\left(P_i^{\frac{1}{2}}\right)+\lambda_{\min}\left({Q_i^*}^{\frac{1}{2}}\right)} \geq \beta_i \geq \frac{2\lambda_{\max}(P_i)^{\frac{3}{2}}\rho}{\epsilon_i\lambda_{\min}(Q_i^*)}$, if the cooperation matrices Q_{ji} satisfies

$$\sum_{j\in\mathscr{N}_i}\lambda_{\max}(Q_{ji}) < \frac{\epsilon_i^2\frac{\lambda_{\min}(Q_i)}{\lambda_{\max}(P_i)} - \mathscr{B}_i}{\mathscr{C}_j}, \quad (25)$$

where $\mathscr{B}_i$ and $\mathscr{C}_j$ are defined as:

$$\begin{aligned}\mathscr{B}_i \triangleq &\sum_{n=1}^{N_p-1}\left[\left({L_f}_i^{n-1}\rho\lambda_{\max}\left(Q_i^{\frac{1}{2}}\right) + 2\left(1-\frac{n}{N_p}\zeta_i\right)\mathscr{c}_i\right)\right.\\ &\left.\times\left({L_f}_i^{n-1}\rho\lambda_{\max}\left(Q_i^{\frac{1}{2}}\right)\right)\right],\\ \mathscr{C}_j \triangleq &\sum_{n=0}^{-k_S+N_p-1}\sum_{j\in\mathscr{N}_i}\left[\left(\mathscr{c}_i + \mathscr{c}_j - \frac{n+1}{N_p}(\zeta_j\mathscr{c}_j + \zeta_i\mathscr{c}_i)\right.\right.\\ &\left.\left.-\frac{k_S}{N_p}\zeta_j\mathscr{c}_j\right) + {L_f}_i^{n}\rho\right]^2\\ &+\sum_{n=-k_S+N_p}^{N_p-1}\sum_{j\in\mathscr{N}_i}\\ &\left[\frac{\xi_j\epsilon_j}{\lambda_{\min}\left({P_j}^{\frac{1}{2}}\right)} + \left(1-\frac{n+1}{N_p}\zeta_i\right)\mathscr{c}_i + {L_f}_i^{n}\rho\right]^2\\ &+\sum_{j\in\mathscr{N}_i}\left(\frac{\epsilon_j}{\lambda_{\min}\left({P_j}^{\frac{1}{2}}\right)} + \frac{\xi_i\epsilon_i}{\lambda_{\min}\left({P_i}^{\frac{1}{2}}\right)}\right)^2.\end{aligned}$$

Here, ζ_i, ζ_j, ξ_i, and ξ_j are the designed parameters which satisfy the conditions in Theorem 1, then the overall system state will converge to the convergence set $\Omega_1^* \times \Omega_2^* \times \cdots \times \Omega_M^*$, where $\Omega_i^* \triangleq \{x_i | {x_i}^{\mathrm{T}}P_i x_i \leq (1+\frac{\lambda_{\min}(Q_i^*)}{\lambda_{\max}(P_i)})\beta_i{\epsilon_i}^2\}$.

Proof: At the time instant $k+1$, construct the cost function with the candidate input sequence and the predicted state sequence for agent i, $i \in \mathscr{M}$. Then, the difference of the cost function between the two adjacent time instants can be represented as:

$$\begin{aligned}\triangle(J_i) \triangleq\ &J_i\left(\widetilde{x}_i(k_{n+1}|k_1), \widetilde{u}_i(k_{n+1}|k_1), \widetilde{x}^a_{-i}(k_{n+1}|k_1)\right)\\ &- J_i\left(\widehat{x}_i^*(k_n|k), u_i^*(k_n|k), \widehat{x}^a_{-i}(k_n|k)\right),\ n \in \mathbb{N}_{[0,\,N_p-1]}.\end{aligned}$$

We then split $\triangle(J_i)$ with three time intervals:

$$\begin{aligned}\triangle(J_i) &= \mathscr{T}_1 + \mathscr{T}_2 + \mathscr{T}_3\\ &= \sum_{n=1}^{N_p-1}\{\|\widetilde{x}_i(k_n|k_1)\|_{Q_i}^2 + \|\widetilde{u}_i(k_n|k_1)\|_{R_i}^2\\ &\quad -\|\widehat{x}_i^*(k_n|k)\|_{Q_i}^2 - \|u_i^*(k_n|k)\|_{R_i}^2\}\\ &\quad + \|\widetilde{x}_i(k_{N_p}|k_1)\|_{Q_i}^2 + \|\widetilde{u}_i(k_{N_p}|k_1)\|_{R_i}^2\\ &\quad - \|\widehat{x}_i^*(k|k)\|_{Q_i}^2 - \|u_i^*(k|k)\|_{R_i}^2\\ &\quad + \|\widetilde{x}_i(k_{N_p+1}|k_1)\|_{P_i}^2 - \|\widehat{x}_i^*(k_{N_p}|k)\|_{P_i}^2\end{aligned}$$

$$
\begin{aligned}
&+\sum_{n=0}^{N_p-1}\sum_{j\in\mathcal{N}_i}\|\widetilde{x}_i(k_{n+1}|k_1)-\widehat{x}^a_{-i}(k_{n+1}|k_1)\|^2_{Q_{ji}}\\
&-\sum_{n=0}^{N_p-1}\sum_{j\in\mathcal{N}_i}\|\widetilde{x}_i(k_n|k)-\widehat{x}^a_{-i}(k_n|k)\|^2_{Q_{ji}}.
\end{aligned}
$$

On the right-hand side of this equation, the first part can be bounded as

$$
\begin{aligned}
\mathscr{T}_1 =& \sum_{n=1}^{N_p-1}\left\{\|\widetilde{x}_i(k_n|k_1)\|^2_{Q_i}+\|\widetilde{u}_i(k_n|k_1)\|^2_{R_i}\right.\\
&\left.-\|\widehat{x}^*_i(k_n|k)\|^2_{Q_i}-\|u^*_i(k_n|k)\|^2_{R_i}\right\}\\
\overset{(15)}{=}& \sum_{n=1}^{N_p-1}\|\widetilde{x}_i(k_n|k_1)\|^2_{Q_i}-\|\widehat{x}^*_i(k_n|k)\|^2_{Q_i}\\
\leq& \sum_{n=1}^{N_p-1}\left(\|\widetilde{x}_i(k_n|k_1)\|_{Q_i}+\|\widehat{x}^*_i(k_n|k)\|_{Q_i}\right)\\
&\times\|\widetilde{x}_i(k_n|k_1)-\widehat{x}^*_i(k_n|k)\|_{Q_i}\\
\leq& \sum_{n=1}^{N_p-1}\left\{\left({L_{fi}}^{n-1}\rho\lambda_{\max}\left(Q_i^{\frac{1}{2}}\right)+2\left(1-\frac{n}{N_p}\zeta_i\right)c_i\right)\right.\\
&\left.\times\left({L_{fi}}^{n-1}\rho\lambda_{\max}\left(Q_i^{\frac{1}{2}}\right)\right)\right\}.
\end{aligned}
$$

For the second part

$$
\begin{aligned}
\mathscr{T}_2 =& \|\widetilde{x}_i(k_{N_p}|k_1)\|^2_{Q_i}+\|\widetilde{u}_i(k_{N_p}|k_1)\|^2_{R_i}\\
&+\|\widetilde{x}_i(k_{N_p+1}|k_1)\|^2_{P_i}-\|\widehat{x}^*_i(k_{N_p}|k)\|^2_{P_i},
\end{aligned}
\tag{26}
$$

it is proven that the candidate state at the time instant $k+N_p$ enters the terminal region. According to *Assumption 3*, the following inequality holds true:

$$
\begin{aligned}
&\|\widehat{x}^*_i(k_{N_p}|k)\|^2_{P_i}-\|\widetilde{x}_i(k_{N_p+1}|k_1)\|^2_{P_i}\\
&\geq\|\widehat{x}_i(k_{N_p})\|^2_{Q^*_i}=\|\widetilde{x}_i(k_{N_p}|k_1)\|^2_{Q_i}+\|\widetilde{u}_i(k_{N_p}|k_1)\|^2_{R_i},
\end{aligned}
$$

which means $\mathscr{T}_2\leq 0$.

The third part can be evaluated as follows:

$$
\begin{aligned}
&\mathscr{T}_3 =\\
&\sum_{n=0}^{N_p-1}\sum_{j\in\mathcal{N}_i}\|\widetilde{x}_i(k_{n+1}|k_1)-\widehat{x}^a_j(k_{n+1}|k_1)\|^2_{Q_{ji}}\\
&-\sum_{n=0}^{N_p-1}\sum_{j\in\mathcal{N}_i}\|\widehat{x}_i(k_n|k)-\widehat{x}^a_j(k_n|k)\|^2_{Q_{ji}}\\
&\leq\sum_{n=0}^{N_p-1}\sum_{j\in\mathcal{N}_i}\|\widetilde{x}_i(k_{n+1}|k_1)-\widehat{x}^a_j(k_{n+1}|k_1)\|^2_{Q_{ji}}\\
&\leq\sum_{n=0}^{N_p-1}\sum_{j\in\mathcal{N}_i}\left(\|\widetilde{x}_i(k_{n+1}|k_1)\|_{Q_{ji}}+\|\widehat{x}^a_j(k_{n+1}|k_1)\|_{Q_{ji}}\right)^2\\
&=\sum_{n=0}^{-k_S+N_p-1}\sum_{j\in\mathcal{N}_i}\left(\|\widetilde{x}_i(k_{n+1}|k_1)\|_{Q_{ji}}+\|\widehat{x}^a_j(k_{n+1}|k_1)\|_{Q_{ji}}\right)^2\\
&+\sum_{n=-k_S+N_p}^{N_p-2}\sum_{j\in\mathcal{N}_i}\left(\|\widetilde{x}_i(k_{n+1}|k_1)\|_{Q_{ji}}+\|\widehat{x}^a_j(k_{n+1}|k_1)\|_{Q_{ji}}\right)^2\\
&+\sum_{j\in\mathcal{N}_i}\left(\|\widetilde{x}_i(k_{N_p+1}|k_1)\|_{Q_{ji}}+\|\widehat{x}^a_j(k_{N_p+1}|k_1)\|_{Q_{ji}}\right)^2,
\end{aligned}
$$

where $k_S=k-k_{s_{ji}}$.

To evaluate the upper bound of $\mathscr{T}_3$, we can derive the upper bound of each element in the polynomial. Considering the term $\|\widehat{x}^a_j(k_{n+1}|k_1)\|_{Q_{ji}}$, we have:

$$
\begin{aligned}
\|\widehat{x}^a_j(k_{n+1}|k_1)\|_{Q_{ji}}&\overset{(11),(12)}{=\!=\!=}\|\widehat{x}^*_j(k_{n+1}|k_{s_{ji}})\|_{Q_{ji}}\\
&\leq\left(1-\frac{k_S+n+1}{N_p}\zeta_j\right)c_j\lambda_{\max}\left(Q_{ji}^{\frac{1}{2}}\right),
\end{aligned}
$$

with $n\in\mathbb{N}_{[0,-k_S+N_p-1]}$, and

$$
\|\widehat{x}^a_j\left(k_{n+1}|k_1\right)\|_{Q_{ji}}\leq\frac{\lambda_{\max}\left({Q_{ji}}^{\frac{1}{2}}\right)}{\lambda_{\min}\left({P_j}^{\frac{1}{2}}\right)}\xi_j\epsilon_j.
$$

with $n\in\mathbb{N}_{[-k_S+N_p,N_p-1]}$.

Similarly, considering the term $\|\widetilde{x}_i(k_{n+1}|k_1)\|_{Q_{ji}}$, and recalling (21), we can obtain

$$
\begin{aligned}
&\|\widetilde{x}_i(k_{n+1}|k_1)\|_{Q_{ji}}\leq\left\{\|\widehat{x}^*_i(k_{n+1}|k)\|_{Q_{ji}}+{L_{fi}}^n\rho\lambda_{\max}\left(Q_{ji}^{\frac{1}{2}}\right)\right\}\\
&\leq\left\{\left(1-\frac{n+1}{N_p}\zeta_i\right)c_i\lambda_{\max}\left(Q_{ji}^{\frac{1}{2}}\right)+{L_{fi}}^n\rho\lambda_{\max}\left(Q_{ji}^{\frac{1}{2}}\right)\right\},
\end{aligned}
$$

with $n\in\mathbb{N}_{[0,N_p-2]}$, and

$$
\|\widetilde{x}_i(k_{N_p+1}|k_1)\|_{Q_{ji}}\leq\frac{\lambda_{\max}\left({Q_{ji}}^{\frac{1}{2}}\right)}{\lambda_{\min}\left({P_i}^{\frac{1}{2}}\right)}\xi_i\epsilon_i.
$$

Consequently, the upper bound of $\mathscr{T}_3$ can be formulated as:

$$
\begin{aligned}
\mathscr{T}_3\leq&\sum_{n=0}^{-k_S+N_p-1}\sum_{j\in\mathcal{N}_i}\left\{{L_{fi}}^n\rho\lambda_{\max}\left(Q_{ji}^{\frac{1}{2}}\right)\right.\\
&\left.+\left(c_i+c_j-\frac{n+1}{N_p}\left(\zeta_jc_j+\zeta_ic_i\right)-\frac{k_S}{N_p}\zeta_jc_j\right)\lambda_{\max}\left(Q_{ji}^{\frac{1}{2}}\right)\right\}^2\\
&+\sum_{n=-k_S+N_p}^{N_p-1}\sum_{j\in\mathcal{N}_i}\left\{\frac{\lambda_{\max}\left({Q_{ji}}^{\frac{1}{2}}\right)}{\lambda_{\min}\left({P_j}^{\frac{1}{2}}\right)}\xi_j\epsilon_j+{L_{fi}}^n\rho\lambda_{\max}\left(Q_{ji}^{\frac{1}{2}}\right)\right.\\
&\left.+\left(1-\frac{n+1}{N_p}\zeta_i\right)c_i\lambda_{\max}\left(Q_{ji}^{\frac{1}{2}}\right)\right\}^2\\
&+\sum_{j\in\mathcal{N}_i}\left(\frac{\lambda_{\max}({Q_{ji}}^{\frac{1}{2}})}{\lambda_{\min}\left({P_j}^{\frac{1}{2}}\right)}\epsilon_j+\frac{\lambda_{\max}\left({Q_{ji}}^{\frac{1}{2}}\right)}{\lambda_{\min}\left({P_i}^{\frac{1}{2}}\right)}\xi_i\epsilon_i\right)^2
\end{aligned}
$$

$$\triangleq \sum_{j\in\mathscr{N}_i} \lambda_{\max}(Q_{ji})\mathscr{C}_j.$$

To sum up, we can derive that

$$\begin{aligned}\triangle(J_i) &= \mathscr{T}_1 + \mathscr{T}_2 + \mathscr{T}_3 - \|\widehat{x}_i^*(k|k)\|_{Q_i}^2 - \|u_i^*(k|k)\|_{R_i}^2 \\ &\le \mathscr{T}_1 + \mathscr{T}_3 - \|\widehat{x}_i^*(k|k)\|_{Q_i}^2. \end{aligned} \tag{27}$$

Since $\widehat{x}_i^*(k|k) = x_i(k)$, according to 25, the following inequality is satisfied:

$$\mathscr{T}_1 + \mathscr{T}_3 < \epsilon_i^2 \frac{\lambda_{\min}(Q_i)}{\lambda_{\max}(P_i)} \le \|\widehat{x}_i^*(k|k)\|_{Q_i}^2. \tag{28}$$

when $x_i \notin \widehat{\Omega}_i$.

Therefore, it is shown in (28) that the state x_i can be steered into the terminal region $\widehat{\Omega}_i$.

Based on the discussion above, if the largest eigenvalues of Q_{ji} satisfy (25), the states of all agents will be steered into the terminal region by solving the optimization problem $\mathscr{P}_i$. In the following steps, we can prove that the state of each agent will converge to the region $\Omega_i \triangleq \{x_i^{\mathrm{T}} P_i x_i \le \beta_i {\epsilon_i}^2\}$, where $\beta_i \ge \frac{2\lambda_{\max}(P_i{}^{\frac{3}{2}})\rho}{\epsilon_i \lambda_{\min}(Q_i^*)}$. Assume that there exist a constant $\eta_i \in (\sqrt{\beta_i}, 1)$ and a region $\Omega_i^{\eta_i} \triangleq \{x|{x_i}^{\mathrm{T}} P_i x_i \le {\eta_i}^2 {\epsilon_i}^2\}$.

When the state of agent i has entered $\widehat{\Omega}_i$ but has not entered $\Omega_i^{\eta_i}$, we have:

$$\begin{aligned} &{x_i}^{\mathrm{T}}(k+1)P_i x_i(k+1) - {x_i}^{\mathrm{T}}(k)P_i x_i(k) \\ \le& -\|\widehat{x}_i^*(k|k)\|_{Q_i^*}^2 + 2\widehat{x}_i^*(k|k)^{\mathrm{T}} P_i \omega_i(k) \\ \le& -\frac{\lambda_{\min}(Q_i^*)}{\lambda_{\max}(P_i)} {\eta_i}^2 {\epsilon_i}^2 + 2\epsilon_i \lambda_{\max}\left(P_i{}^{\frac{1}{2}}\right)\rho \\ \le& \left(-\eta^2 + \beta_i\right)\frac{\lambda_{\min}(Q_i^*)}{\lambda_{\max}(P_i)}\epsilon_i^2. \end{aligned} \tag{29}$$

Since $\eta_i \in (\sqrt{\beta_i}, 1)$, it can be concluded that when $x_i \notin \Omega_i^{\eta_i}$, the difference between two adjacent time instants of the Lyapunov function designed for the system is always negative, which implies that the state of each agent will converge to the region Ω_i in finite time.

Furthermore, we need to prove that the state will not leave Ω_i^*. Let $\mathscr{K}_i$ be the set of all the time instants that the state of agent enters Ω_i, with $\kappa_i \in \mathscr{K}_i$ being an arbitrary time instant in this set. It can be obtained that:

$${x_i}^{\mathrm{T}}(\kappa_i)P_i x_i(\kappa_i) \le \beta_i {\epsilon_i}^2.$$

Suppose that at time instant $\kappa_i + 1$, the state x_i leaves the region Ω_i. Therefore, based on (29), the following inequality will hold true:

$$\begin{aligned} {x_i}^{\mathrm{T}}(\kappa_i+1)P_i x_i(\kappa_i+1) &\le {x_i}^{\mathrm{T}}(\kappa_i)P_i x_i(\kappa_i) + \beta_i \frac{\lambda_{\min}(Q_i^*)}{\lambda_{\max}(P_i)}\epsilon_i^2 \\ &\le \left(1 + \frac{\lambda_{\min}(Q_i^*)}{\lambda_{\max}(P_i)}\right)\beta_i {\epsilon_i}^2. \end{aligned}$$

which implies $x_i(\kappa_i + 1) \in \Omega_i^*$.

Since $\Omega_i \subset \Omega_i^*$, according to (29), the state of agent i will then converge to Ω_i in finite time. Consequently, the state of agent i, $i \in \mathscr{M}$ will be confined in the small region Ω_i^*, which also implies that the overall system state will converge to the convergence set $\Omega_1^* \times \Omega_2^* \times \cdots \times \Omega_M^*$. ■

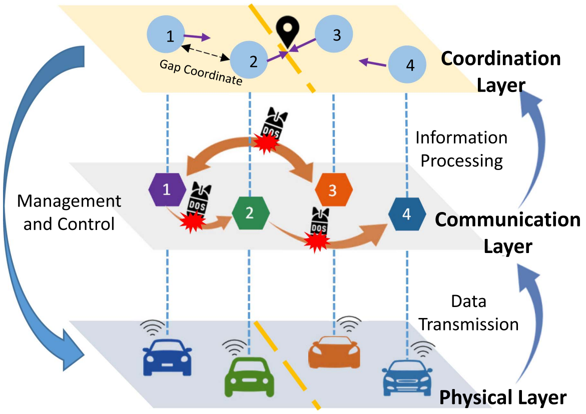


Fig. 3. Cooperative regulation problem for a CPS consisting of four ground vehicles.

Remark 5: Inequality (25) shows the upper bound of the eigenvalues of matrix Q_{ji}. In fact, the disturbance bound can also influence the selection of Q_{ji}. Specifically, larger eigenvalues of matrix Q_{ji} mean lesser tolerance to the disturbance on the agent i. Therefore, we are motivated to propose anther kind of robustness constraint to enhance the robustness against DoS attacks and the external disturbances with slight sacrifice to the region of attraction. To achieve this purpose, the tightened state constraint (9d) and the tightened terminal constraint (9e) can be fused into one constraint, which is represented as $\|\widehat{x}_i(k_n|k)\|_{P_i} \le \Xi(\xi_i, n)$, where $\Xi(\xi_i, n) \triangleq (1 - \frac{n}{N_p})\mathscr{c}_i \xi_i \lambda_{\min}(P_i{}^{\frac{1}{2}}) + \frac{n}{N_p}\xi_i\epsilon_i,\ n \in \mathbb{N}_{[0,\,N_p]}$. In this way, the conditions in Theorem 1 and Theorem 2 can be modified as $\frac{N_p \lambda_{\max}(P_i^{\frac{1}{2}}) L_{fi}{}^{N_p-1}\rho}{\xi_i\epsilon_i + \xi_i \mathscr{c}_i \lambda_{\max}(P_i^{\frac{1}{2}})} \le \xi_i \le \frac{\epsilon_i - \rho\lambda_{\max}(P_i^{\frac{1}{2}}) L_{fi}{}^{N_p-1}}{\epsilon_i}$, and $\mathscr{C}_j \le \sum_{j\in\mathscr{N}_i}\{\sum_{n=0}^{N_p-1}[\Xi(\xi_i,(n+1)) + \Xi(\xi_j,(n+1)) + L_{fj}{}^n\rho]^2 + (\frac{\lambda_{\max}(Q_{ji}{}^{\frac{1}{2}})}{\lambda_{\min}\left(P_j{}^{\frac{1}{2}}\right)}\epsilon_j + \frac{\lambda_{\max}(Q_{ji}{}^{\frac{1}{2}})}{\lambda_{\min}(P_i{}^{\frac{1}{2}})}\xi_i\epsilon_i)^2\}$, thereby enhancing the robustness. In summary, the selection of different types of robustness constraint can be seen as a trade-off between the robustness and the size of the region of attraction.

V. Simulation Study

In this section, we consider a CPS comprising four ground vehicles to test the performance of the proposed approach. As shown in Fig. 3, this multi-agent CPS has a hierarchical architecture consisting of a physical, communication, and coordination layers. Each vehicle in the physical layer has a communication module in the network layer with the communication topology $\mathscr{N}_1 = \{3\}$, $\mathscr{N}_2 = \{1\}$, $\mathscr{N}_3 = \{1\}$, and $\mathscr{N}_4 = \{2\}$. In the meantime, DoS attacks will affect the communication among these communication modules in a random manner, to block each vehicle from receiving information from its neighbors, leading to degraded cooperative regulation performance. To guarantee the performance under DoS attacks and the disturbances on each

TABLE I
PARAMETERS OF THE FOUR VEHICLES

Vehicle Index	M_i (kg)	C_i $(\mathrm{N}\cdot\mathrm{s}^2\cdot\mathrm{m}^{-2})$	R_i (m)
1	1000	0.99	0.30
2	1200	1.1	0.38
3	1500	1.3	0.39
4	1400	1.2	0.37

vehicle, we apply the proposed robust and resilient distributed MPC strategy to this system.

A. System Model and Parameter Configuration

In this article, we only consider the vehicle longitudinal dynamics as adopted in [36]. For the purpose of striking a balance between accuracy and conciseness, the following assumptions have been made: 1) the vehicle body is rigid and strictly left-right symmetric; 2) no tire slip in the longitudinal direction; 3) the driving and braking torques are integrated to one general torque. With the assumptions above, the vehicle i, $i \in \mathscr{M}$ in this system has the nonlinear dynamic model, which is given by:

$$\begin{cases} s_i(k+1) = s_i(k) + T_c v_i(k) \\ v_i(k+1) = v_i(k) + \frac{T_c}{M_i}\left(\frac{T_i(k)}{R_i} - F_i\left(v_i(k)\right)\right) + w_i(k) \end{cases},$$

where $T_c = 0.3$ s is the sampling period; $x_i(k) = [s_i(k), v_i(k)]^{\mathrm{T}}$ is the system state; $s_i(k)$ and $v_i(k)$ represent the position and velocity of vehicle i, respectively; M_i is the vehicle mass; $T_i(k)$ is the integrated driving/braking torque; R_i is the tire radius; $F_i(v_i(k)) = C_i {v_i}^2(k)$ denotes these aerodynamic drag, where C_i is a aerodynamic coefficient. The vehicle coefficients are shown in the Table I. To simplify the algorithm, let $u_i(k) = \frac{T_i(k)}{M_i R_i}$ be the control input. Hence, the integrated torque $T_i(k)$ for each vehicle can be derived through a simple linear transformation after deriving the control input $u_i(k)$. The state constraint for each vehicle is assumed to be same, which is given by $\mathbb{X}_i = \{[s_i, v_i]^{\mathrm{T}} | -1.5\,\mathrm{m} \le s_i \le 1.5\,\mathrm{m}, -1.5\,\mathrm{m/s} \le v_i \le 1.5\,\mathrm{m/s}\}$; the torque constraints are given as $\mathbb{U}_1 = \{T_1| -1300\,\mathrm{N} \le T_1 \le 1300\,\mathrm{N}\}$. $\mathbb{U}_2 = \{T_2| -2000\,\mathrm{N} \le T_2 \le 2000\,\mathrm{N}\}$, $\mathbb{U}_3 = \{T_3| -2500\,\mathrm{N} \le T_3 \le 2500\,\mathrm{N}\}$, and $\mathbb{U}_4 = \{T_4| -2300\,\mathrm{N} \le T_4 \le 2300\,\mathrm{N}\}$, respectively; the disturbances in the four agents are $w_1(k) = 0.0015\sin(\frac{\pi k}{15})$, $w_2(k) = 0.0015\cos(\frac{\pi k}{10})$, $w_3(k) = 0.0015\cos(\frac{\pi k}{5})$, and $w_4(k) = 0.0015\cos(\frac{\pi k}{5} - \frac{\pi}{4})$, respectively. The initial states of the three agents are set as $x_1(0) = [-0.95, -0.3]^{\mathrm{T}}$, $x_2(0) = [-1.4, 0.1]^{\mathrm{T}}$, $x_3(0) = [-1.1, -1.2]^{\mathrm{T}}$, and $x_4(0) = [-1.0, -1.3]^{\mathrm{T}}$ respectively. In the meantime, DoS attacks are set as occurring on all the communication channels among agents at arbitrary time instants, and the launching time of DoS attacks in this simulation is illustrated in Fig. 4.

The design parameters for the proposed robust and resilient distributed MPC algorithm are given in the following. The prediction horizon is set as $N_p = 10$; the weighting matrices Q_1, Q_2, Q_3, and Q_4 are set as [1.1, 0; 0, 1.1], with R_1, R_2, R_3 and R_4 being 1. The corresponding feedback control gain K_i is designed as $K_1 = K_2 = K_3 = K_4 = [0.80, 1.62]$; According to *Assumption 3*, the terminal penalty matrices are derived as $P_1 = P_2 = P_3 = P_4 = [2.23, 0.63; 0.63, 4.69]$. Under these circumstances, the terminal region levels are derived as $\epsilon_1 = \epsilon_2 = \epsilon_3 = \epsilon_4 = 0.70$. Based on [37], the Lipschitz constants L_{f_i} are calculated as $L_{f_1} = 1.17, L_{f_2} = 1.17, L_{f_3} = 1.16$, and $L_{f_4} = 1.16$, respectively. Furthermore, by following the presented sufficient conditions in $Theorem 1$, we can choose the scaling parameters: $\zeta_i = 0.25$ and $\xi_i = 0.91$. In this simulation, the cooperation matrix Q_{ij} are designed as $Q_{12} = Q_{13} = Q_{31} = Q_{24} = [0.022,\ 0;\ 0,\ 0.022]$.

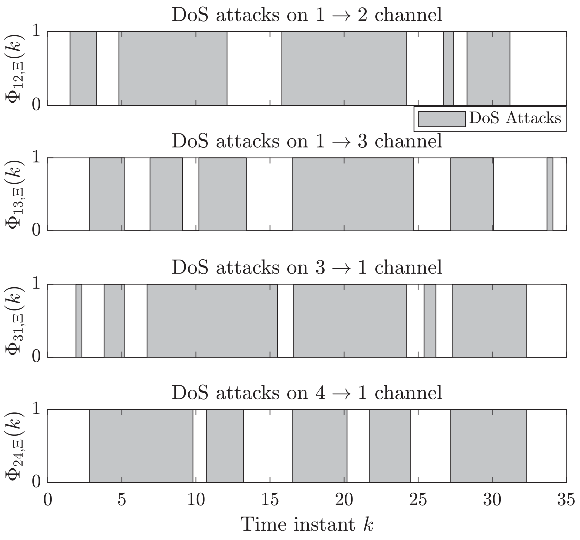


Fig. 4. Launching time of DoS attacks.

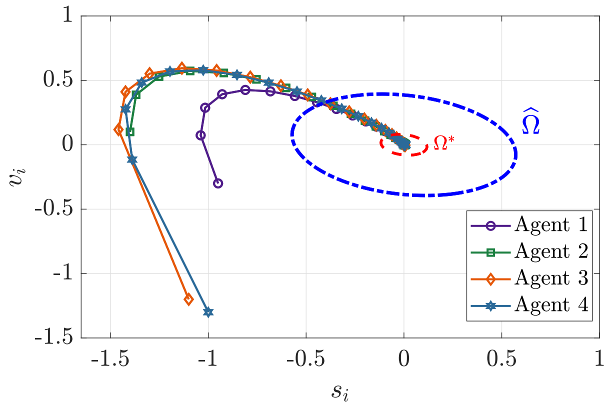


Fig. 5. State trajectories of the CPS.

B. Simulation Results Analysis

The optimization problem $\mathscr{P}_i$ is solved with the nonlinear programming solver IPOPT [38] via the YALMIP [39] toolbox in MATLAB. The state trajectories of the cooperative regulation problem of this multi-agent CPS are demonstrated in Fig. 5. It can be observed that the states of this multi-agent CPS are finally steered into the region $\Omega_1^* \times \Omega_2^* \times \Omega_3^* \times \Omega_4^*$, which verifies the Theorem 2. Furthermore, Fig. 6 illustrates the torque input sequences for the four subsystems, respectively. Based on the results above, it can be verified that the proposed robust and resilient distributed MPC strategy can achieve the cooperation regulation goal with guaranteed input constraint satisfaction under randomly existing DoS attacks.

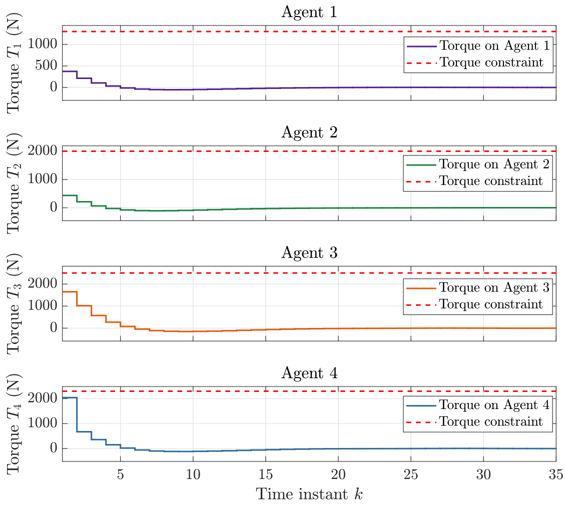


Fig. 6. Integrated torques for four ground vehicles.

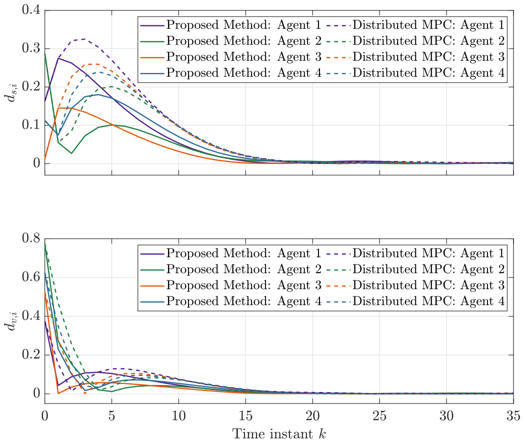


Fig. 7. Deviation between each state and the center of all vehicles.

For the purpose of verifying the effectiveness, the proposed method is compared with the standard distributed MPC method [40] in simulation. To make a fair comparison, we choose the same control parameters for both distributed MPC methods. To guarantee the implementation of the distributed MPC method, we set each controller in this system to use all zero sequences to represent the neigbors' states when attacks occur on this channel. To further show the effectiveness of the proposed method, we compare the deviation between the actual state and the center of the system generated by using the distributed MPC method with robustness constraint and the proposed method, respectively. The result is shown in Fig. 7.

Let $s_a(k) = \frac{1}{M}\sum_{i=1}^{M} s_i$ and $v_a(k) = \frac{1}{M}\sum_{i=1}^{M} v_i$ be the average of the position and the velocity of the four vehicles. Then we can introduce $d_{s,i}(k)$ and $d_{v,i}(k)$ to be the deviation between each state and the center of the system, respectively. With the definition above, these indexes are calculated as:

$$d_{s,i}(k) = \|s_i(k) - s_a(k)\|,\ d_{v,i}(k) = \|v_i(k) - v_a(k)\|.$$

Fig. 7 shows the deviation comparison result between the proposed method and the distributed MPC method with robustness constraint. It can be observed that the proposed method accelerates the speed of convergence under the DoS attacks. To conclude, by applying the robust and resilient distributed MPC control strategy, the states of the multi-agent CPS can be steered into the region $\Omega_1^* \times \Omega_2^* \times \Omega_3^* \times \Omega_4^*$ under the bounded disturbance and randomly occurring DoS attacks, which meets the theoretical analysis in IV.

VI. Conclusion

In this work, we have developed the robust and resilient distributed MPC framework for discrete-time nonlinear multi-agent CPS subject to external disturbances and randomly occurring DoS attacks to achieve the cooperative regulation goal. A new type of robustness constraint approach is proposed to enhance the robustness of the MPC algorithm while also enlarging the region of attraction compared to the original one. Furthermore, a lengthened sequence transmission strategy is also applied to utilize and lengthen the predicted state and control input sequences to mitigate the information block out among the agents induced by DoS attacks. We have proven that the proposed algorithm is recursively feasible and the state of the closed-loop multi-agent CPS can be steered into a small region containing the equilibrium. Numerical results also show the advantages of the proposed work. Future work will focus on expanding the region of attraction of this method.

References

[1] K. Zhang, Y. Shi, S. Karnouskos, T. Sauter, H. Fang, and A. W. Colombo, "Advancements in industrial cyber-physical systems: An overview and perspectives," *IEEE Trans. Ind. Inform.*, vol. 19, no. 1, pp. 716–729, Jan. 2023.

[2] A. W. Colombo, S. Karnouskos, O. Kaynak, Y. Shi, and S. Yin, "Industrial cyberphysical systems: A backbone of the fourth industrial revolution," *IEEE Ind. Electron. Mag.*, vol. 11, no. 1, pp. 6–16, Mar. 2017.

[3] K.-D. Kim and P. R. Kumar, "Cyber–physical systems: A perspective at the centennial," *Proc. IEEE*, vol. 100, no. Special Centennial Issue, pp. 1287–1308, May 2012.

[4] R. Owoputi and S. Ray, "Security of multi-agent cyber-physical systems: A survey," *IEEE Access*, vol. 10, pp. 121465–121479, Nov. 2022.

[5] A. Dorri, S. S. Kanhere, and R. Jurdak, "Multi-agent systems: A survey," *IEEE Access*, vol. 6, pp. 28573–28593, Apr. 2018.

[6] H. Cai and J. Huang, "Leader-following adaptive consensus of multiple uncertain rigid spacecraft systems," *Sci. China Inf. Sci.*, vol. 59, no. 1, pp. 1–13, Jan. 2016.

[7] Z. Feng, C. Sun, and G. Hu, "Robust connectivity preserving rendezvous of multirobot systems under unknown dynamics and disturbances," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 4, pp. 725–735, Dec. 2017.

[8] P. Liu, A. Kurt, and U. Ozguner, "Distributed model predictive control for cooperative and flexible vehicle platooning," *IEEE Trans. Control Syst. Technol.*, vol. 27, no. 3, pp. 1115–1128, May 2019.

[9] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Proc. Hybrid Syst.: Comput. Control: 12th Int. Conf.*, 2009, pp. 31–45.

[10] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," *IEEE Internet Comput.*, vol. 10, no. 1, pp. 82–89, Jan. 2006.

[11] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[12] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. IEEE 47th Annu. Allerton Conf. Commun., Control, Comput.*, 2009, pp. 911–918.

[13] J. Chen and Y. Shi, "Stochastic model predictive control framework for resilient cyber-physical systems: Review and perspectives," *Philos. Trans. Roy. Soc.*, vol. 379, no. 2207, pp. 1–13, Aug. 2021.

[14] Y. Shi and K. Zhang, "Advanced model predictive control framework for autonomous intelligent mechatronic systems: A tutorial overview and perspectives," *Annu. Rev. Control*, vol. 52, pp. 170–196, Nov. 2021.

[15] Q. Sun, K. Zhang, and Y. Shi, "Resilient model predictive control of cyber–physical systems under DoS attacks," *IEEE Trans. Ind. Inform.*, vol. 16, no. 7, pp. 4920–4927, Jul. 2020.

[16] Y.-C. Sun and G.-H. Yang, "Robust event-triggered model predictive control for cyber-physical systems under denial-of-service attacks," *Int. J. Robust Nonlinear Control*, vol. 29, no. 14, pp. 4797–4811, Jul. 2019.

[17] Q. Sun, J. Chen, and Y. Shi, "Event-triggered robust MPC of nonlinear cyber-physical systems against DoS attacks," *Sci. China Inf. Sci.*, vol. 65, no. 1, pp. 1–17, Jan. 2022.

[18] N. He, K. Ma, and H. Li, "Resilient predictive control strategy of cyber–physical systems against FDI attack," *IET Control Theory Appl.*, vol. 16, no. 11, pp. 1098–1109, Apr. 2022.

[19] G. Franzè, F. Tedesco, and W. Lucia, "Resilient control for cyber-physical systems subject to replay attacks," *IEEE Control Syst. Lett.*, vol. 3, no. 4, pp. 984–989, Oct. 2019.

[20] B. Li, X. Zhou, Z. Ning, X. Guan, and K.-F. C. Yiu, "Dynamic event-triggered security control for networked control systems with cyber-attacks: A model predictive control approach," *Inf. Sci.*, vol. 612, pp. 384–398, Oct. 2022.

[21] T. Arauz, P. Chanfreut, and J. Maestre, "Cyber-security in networked and distributed model predictive control," *Annu. Rev. Control*, vol. 53, pp. 338–355, May 2022.

[22] A. Liu and L. Bai, "Distributed model predictive control for wide area measurement power systems under malicious attacks," *IET Cyber-Physical Syst.: Theory Appl.*, vol. 3, no. 3, pp. 111–118, Feb. 2018.

[23] G. Franzè, F. Tedesco, and D. Famularo, "Resilience against replay attacks: A distributed model predictive control scheme for networked multi-agent systems," *IEEE/CAA J. Automatica Sinica*, vol. 8, no. 3, pp. 628–640, Mar. 2021.

[24] H. Yang, Y. Li, L. Dai, and Y. Xia, "MPC-based defense strategy for distributed networked control systems under DoS attacks," *Syst. Control Lett.*, vol. 128, pp. 9–18, May 2019.

[25] L. Qiu, L. Dai, U. Ahsan, C. Fang, M. Najariyan, and J. F. Pan, "Model predictive control for networked multiple linear motors system under DoS attack and time delay," *IEEE Trans. Ind. Inform.*, vol. 19, no. 1, pp. 790–799, Jan. 2023.

[26] M. H. Basiri, N. L. Azad, and S. Fischmeister, "Attack resilient heterogeneous vehicle platooning using secure distributed nonlinear model predictive control," in *Proc. IEEE 28th Mediterranean Conf. Control Automat.*, 2020, pp. 307–312.

[27] J. Chen, H. Zhang, and G. Yin, "Distributed dynamic event-triggered secure model predictive control of vehicle platoon against DoS attacks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 3, pp. 2863–2877, Mar. 2023.

[28] H. Li and Y. Shi, "Robust distributed model predictive control of constrained continuous-time nonlinear systems: A robustness constraint approach," *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1673–1678, Jun. 2014.

[29] H. Li and Y. Shi, *Robust Receding Horizon Control for Networked and Distributed Nonlinear Systems*. Berlin, Germany: Springer, 2017.

[30] H. Li and Y. Shi, "Distributed receding horizon control of large-scale nonlinear systems: Handling communication delays and disturbances," *Automatica*, vol. 50, no. 4, pp. 1264–1271, Apr. 2014.

[31] G. Pin, D. M. Raimondo, L. Magni, and T. Parisini, "Robust model predictive control of nonlinear systems with bounded and state-dependent uncertainties," *IEEE Trans. Autom. Control*, vol. 54, no. 7, pp. 1681–1687, Jul. 2009.

[32] T. Parisini, M. Sanguineti, and R. Zoppoli, "Nonlinear stabilization by receding-horizon neural regulators," *Int. J. Control*, vol. 70, no. 3, pp. 341–362, 1998.

[33] A. Cetinkaya, K. Kikuchi, T. Hayakawa, and H. Ishii, "Randomized transmission protocols for protection against jamming attacks in multi-agent consensus," *Automatica*, vol. 117, Jul. 2020.

[34] H. Michalska and D. Q. Mayne, "Robust receding horizon control of constrained nonlinear systems," *IEEE Trans. Autom. Control*, vol. 38, no. 11, pp. 1623–1633, Nov. 1993.

[35] W. B. Dunbar, "Distributed receding horizon control of dynamically coupled nonlinear systems," *IEEE Trans. Autom. Control*, vol. 52, no. 7, pp. 1249–1263, Jul. 2007.

[36] Y. Zheng, S. E. Li, K. Li, F. Borrelli, and J. K. Hedrick, "Distributed model predictive control for heterogeneous vehicle platoons under unidirectional topologies," *IEEE Trans. Control Syst. Technol.*, vol. 25, no. 3, pp. 899–910, May 2017.

[37] H. Khalil, *Nonlinear Systems* (Pearson Education Series). Hoboken, NJ, USA: Prentice Hall, 2000.

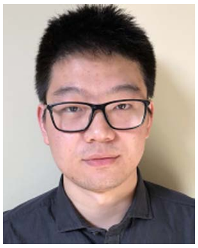
[38] A. Wächter and L. Biegler, "On the implementation of an interior-point filter line-search algorithm for large-scale nonlinear programming," *Math. Program.*, vol. 106, pp. 25–57, Apr. 2005.

[39] J. Lofberg, "YALMIP: A toolbox for modeling and optimization in MATLAB," in *Proc. IEEE Int. Conf. Robot. Automat.*, 2004, pp. 284–289.

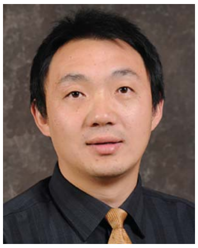
[40] E. Camponogara, D. Jia, B. Krogh, and S. Talukdar, "Distributed model predictive control," *IEEE Control Syst. Mag.*, vol. 22, no. 1, pp. 44–52, Feb. 2002.

Yufan Dai (Graduate Student Member, IEEE) received the B.Sc. degree from the School of Physics and Technology from Wuhan University, Wuhan, China, in 2020. He is currently working toward the M.A.Sc. degree with the Department of Mechanical Engineering, University of Victoria, Victoria, BC, Canada. His main research interests include model predictive control, cyber-physical systems, and resilient control.

Manyun Li is currently a high school student (Class 2024) with the Basis International School Parklane Harbor, Huizhou, China. Since June 2022, she has been a part-time research student with the Applied Control and Information Processing Lab, University of Victoria, Victoria, BC, Canada. Her research interests include control engineering and intelligent autonomous systems.



Kunwu Zhang (Member, IEEE) received the M.A.Sc. and Ph.D. degrees in mechanical engineering from the University of Victoria, Victoria, BC, Canada, in 2016 and 2021, respectively. Since January 2022, he has been a Postdoctoral Researcher with the Department of Mechanical Engineering, University of Victoria. His research interests include adaptive control, model predictive control, optimization, and robotic systems.



Yang Shi (Fellow, IEEE), received the Ph.D. degree in electrical and computer engineering from the University of Alberta, Edmonton, AB, Canada, in 2005. From 2005 to 2009, he was an Assistant Professor and an Associate Professor with the Department of Mechanical Engineering, University of Saskatchewan, Saskatoon, SK, Canada. In 2009, he joined the University of Victoria, Victoria, BC, Canada, where he is currently a Professor with the Department of Mechanical Engineering. He was a Visiting Professor with the University of Tokyo, Tokyo, Japan, in 2013. His research interests include networked and distributed systems, model predictive control, cyber-physical systems, robotics and mechatronics, autonomous systems (AUV and UAV), and energy system applications. Prof. Shi was the recipient of the several teaching awards including the University of Saskatchewan Student Union Teaching Excellence Award in 2007, Faculty of Engineering Teaching Excellence Award in 2012. He was also the recipient of the Craigdarroch Medal for Excellence in Research in 2015 at the University of Victoria, 2017 IEEE Transactions on Fuzzy Systems Outstanding Paper Award, JSPS Invitation Fellowship (short-term), Humboldt Research Fellowship for Experienced Researchers in 2018, and CSME Mechatronics Medal in 2023. Since 2018, he has been a member of the IEEE IES Administrative Committee.During 2022–2023, he was Vice President of IES. During 2018–2022, he was the Chair of IEEE IES Technical Committee on Industrial Cyber–Physical Systems. He is the Co-Editor-in-Chief of the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, and an Associate Editor for *Automatica*, the IEEE TRANSACTIONS ON AUTOMATIC CONTROL, and the IEEE TRANSACTIONS ON CYBERNETICS. He is a Fellow of ASME, CSME, Engineering Institute of Canada, and Canadian Academy of Engineering. He is registered Professional Engineer in British Columbia, Canada.