ISA Transactions 153 (2024) 1–12

Contents lists available at ScienceDirect

ISA Transactions

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

Research article

Dynamic event-triggering-based distributed model predictive control of heterogeneous connected vehicle platoon under DoS attacks

Hao Zeng, Zehua Ye, Dan Zhang *

Research Center of Automation and Artificial Intelligence, Zhejiang University of Technology, Hangzhou, 310023, PR China

ARTICLE INFO

Keywords:
Heterogeneous CVP
DMPC
DoS attacks
DETM
ISPS

ABSTRACT

This paper is concerned with the distributed model predictive control (DMPC) for heterogeneous connected vehicle platoon (CVP) under denial-of-service (DoS) attacks. Firstly, a dynamic event-triggering mechanism (DETM) based on the information interaction between vehicles is proposed to reduce the communication and computational burdens. Due to the fact that the triggering moment for each vehicle cannot be synchronized and DoS attacks can break the communication between vehicles, a packet replenishment mechanism is designed to ensure the integrity and effectiveness of information interaction. Then, the effect of external disturbance is handled by adding robustness constraints to the DMPC algorithm. In addition, the recursive feasibility of the DMPC algorithm and input-to-state practical stability (ISPS) of the CVP control system are demonstrated. Finally, the effectiveness of the algorithm is verified by simulation and comparison results.

1. Introduction

With the development of the economy and technology, the number of vehicles has increased rapidly, raising the probability of traffic congestion and traffic accidents [1]. The control issue of the connected vehicle platoon (CVP) system aims to keep vehicles traveling at a desired longitudinal speed and spacing, which is regarded to be an effective technical solution to solve the above problems [2]. Studies have shown that CVP control can reduce the air resistance of following vehicles during traveling, effectively reduce fuel consumption, and improve the safety of traffic [3,4]. Therefore, the control problem of CVP system has attracted extensive attention in intelligent transport systems. The CVP system uses the IEEE 802.11p protocol for short-range communication and C-V2X/5G technology for long-range communication [5]. In this scenario, the CVP system is a complex cyber–physical system with deep integration of computation, communication, control, and vehicle.

As the CVP system transmits information over networks, cyber-attacks on such vehicles are becoming increasingly prevalent as the growing openness of networks [6,7]. Thus, the security of the CVP system is worth investigating deeply. There are three representative types of cyber-attacks, which can be broadly categorized as deception attacks [8–10], replay attacks [11,12], and denial-of-service (DoS) attacks [13–15]. DoS attacks are the most prevalent and destructive form of cyber-attacks [16,17]. When DoS attacks occur, the adversary occupies the system's communication and storage units by sending numerous illegal request services, which causes the system to be unable to process regular request services sent by legitimate users [18,19]. In this case, DoS attacks can break communication channels in the CVP system, which can degrade the control performance of the CVP system and even lead to collision.

The security control problem of CVP system under DoS attacks has been extensively studied in the past few years. For instance, a sliding mode observer was designed to detect whether DoS attacks occur in [20], and the impact of DoS attacks on CVP system was illustrated through simulation. In [21], a robust event-triggering mechanism (ETM) for the CVP system was designed to mitigate the impact of DoS attacks and reduce the network burden. In [22], a distributed resilient control law was devised for the heterogeneous CVP system under DoS attacks, and the effectiveness of the algorithm was verified through numerical simulations. In [23], a resilient adaptive event-triggering platoon control strategy was proposed for the CVP system under DoS attacks to enable vehicles to maintain the prescribed spacing. In our earlier work [24], the controller design for the CVP system under DoS attacks was analyzed using a switched system method and the effect of DoS attacks parameters on the system's performance. In [25], the security control problem of CVP system under DoS attacks was investigated and the controller gains were calculated based on linear matrix inequalities. In [26], a control protocol based on ETM that can achieve leader-following consensus was proposed, and the effectiveness of the proposed distributed security control protocol was verified by the numerical simulation of CVP system. Although the above results are very effective for CVP system subject to DoS attacks, the constraint

* Corresponding author.
E-mail address: danzhang@zjut.edu.cn (D. Zhang).

https://doi.org/10.1016/j.isatra.2024.07.011
Received 24 February 2024; Received in revised form 11 June 2024; Accepted 5 July 2024
Available online 15 July 2024

problem has yet to be well studied in the above studies. Instead, the parameters of vehicles in the CVP system are usually constrained during traveling, see, e.g., speed and control input. Thus, it is necessary to investigate the resilient control problem of the CVP system in the constrained situation.

Model predictive control (MPC) algorithm represents a viable solution to the issue of control systems that are constrained by inputs and states [27]. The MPC algorithm has been widely applied in various fields, and those comprehensive results on MPC can roughly classify into three types: centralized MPC [28], decentralized MPC [29], and distributed MPC (DMPC) [30–32]. The centralized MPC shows proficient optimization capabilities, but it is only suitable for small-scale systems with low computational requirements. The decentralized MPC reduces the computational burden by eliminating the need for connections between subsystems. However, the performance of the system may be degraded. The DMPC realizes the optimal control of the system by decomposing the large-scale online optimization problem and the information interaction between subsystems, which is proved to be suitable for solving control problems of the large-scale system. Therefore, the DMPC received attractive research attention in the field of the CVP system due to its outstanding performance and capability to deal with constraints efficiently. In [33], a distributed stochastic MPC algorithm was proposed for the vehicle dynamic system with modeling uncertainty, and it was proven that the tracking errors in the CVP system asymptotically converge to zero under that algorithm. In [34], a DMPC algorithm was introduced to address the challenges in multi-agent systems with time-varying communication topology, and the effects of changing communication topology on stability were mitigated efficiently. In [35], two different DMPC algorithms were proposed to ensure the asymptotic stability and string stability of the CVP system under a switched communication topology.

Although the above methods can be adopted to solve the constraint problem in the CVP system, the communication constraint problem has not been well solved. In reality, the communication resource is usually limited for a large-scale vehicle network [36]. The ETM can effectively decrease the volume of processed data while conserving network resources, which has been extensively studied in literature [37–39]. There are two types of ETM: static ETM (SETM) and dynamic ETM (DETM). Compared with the SETM, the DETM can further reduce the number of triggers by introducing dynamic variables. Thus, DETM has a broader application in the CVP system. Recently, a DETM was proposed in [40] to dynamically adjust the threshold parameter by the measurement error, and thereby significantly reducing the communication burden of the CVP system. In [41], a DETM with threshold parameter varying according to vehicle state and bandwidth state was proposed, and simulation results demonstrated the significant reduction in bandwidth consumption achieved by the method. Although the above results effectively reduce the number of triggers, they do not consider the situation where DoS attacks can disrupt communication. Therefore, it is urgent to design a resilient security control algorithm and DETM in order to reduce the communication burden of CVP system under DoS attacks.

On the basis of the above discussion, this paper is concerned with the DETM-based DMPC problem for CVP system under DoS attacks. A heterogeneous CVP system with external disturbance is first established, and a DETM with dynamically adjusted threshold parameters is proposed to save communication resources. Then, sufficient conditions to ensure the feasibility of the DMPC algorithm are given, and the stability of the CVP system under DoS attack is analyzed under the DMPC algorithm. In the section of simulation, a CVP system with six vehicles is finally taken as an example to verify the effectiveness of the designed method. The main contributions of this paper can be summarized as follows:

(1) A new DETM is designed. The threshold parameters of the DETM can be dynamically adjusted by the error between the actual state of the ith vehicle and the predicted state in the buffer. The threshold parameter will decrease as the error between the actual state of the ith vehicle and the predicted state in the buffer becomes larger. In the simulation, the proposed DETM reduces the number of triggers by 46.6% in the time interval $[0, 800]$ compared with the existing DETM. Therefore, the proposed DETM can significantly reduce the number of triggers and network burden.

(2) A DMPC algorithm is proposed. The virtual leading vehicle generates reference state trajectory for the CVP system to obtain the tracking error equation for each vehicle. The effect of external disturbances on the CVP system is handled by adding robust constraints to the tracking error of each vehicle in the DMPC algorithm. The recursive feasibility of DMPC and the input-to-state practical stability (ISPS) of the CVP system are analyzed based on the newly proposed DETM.

(3) A packet replenishment mechanism is designed. The packet replenishment mechanism can ensure the integrity and effectiveness of information interaction under DETM in the presence of DoS attacks. When DoS attacks occur, input packets stored in the buffer are used to control the vehicle. Compared with the zero input mechanism, the hold input mechanism in this paper compensates for the impact of DoS attacks on the CVP system.

Notations: In this paper, R is the set of all real numbers and $R^{m\times n}$ denotes the $m \times n$ dimensional matrix. N^+ denotes the set of non-zero natural numbers, I_m denotes the m-dimensional identity matrix. Define $\|x\|^2 = x^T x$ and $\|x\|_P^2 = x^T P x$, where $x \in R^{m\times 1}$ and $P \in R^{m\times m}$. Define $\lambda_{\max}(P)$ and $\lambda_{\min}(P)$ denote the maximum and minimum eigenvalues of the matrix P.

2. Preliminaries and problem formulation

This section elaborates on some basis and problem description. The system structure is shown in Fig. 1. The data is transmitted according to the communication topology when the event-triggering condition is satisfied. The communication channels will be jammed when DoS attacks occur.

2.1. Communication graph

The CVP system can have many different communication topologies to adapt to the requirements of various application scenarios. The communication interactions among vehicles can be described by graph theory, which can be represented as a directed graph ζ. For ζ, the adjacency matrix $\mathcal{A}_{\mathcal{N}}$ is defined as $\mathcal{A}_{\mathcal{N}} = [a_{ij}] \in R^{\mathcal{N}\times\mathcal{N}} (i, j = 1, 2, \dots, \mathcal{N})$, where $a_{ij} = 1$ represents that the ith vehicle can receive data from the jth vehicle, otherwise $a_{ij} = 0$. Define $\mathbb{C}_i$ as the set of vehicles, where $\mathbb{C}_i = \{j | a_{ij} = 1\}$.

2.2. Vehicle models

A CVP system with $\mathcal{N}$ vehicles is considered in this work. The leading vehicle is indexed as 1, and the following vehicles are indexed from 2 to $\mathcal{N}$. It is assumed that the virtual leading vehicle operates at a fixed speed to generate reference position and speed for the vehicles in the platoon. The discrete-time longitudinal dynamics model of the virtual leading vehicle can be represented as

$$\begin{cases} p_r(k+1) = p_r(k) + v_r(k)\Delta T \\ v_r(k+1) = v_r(k) \\ a_r(k+1) = 0 \end{cases} \tag{1}$$

where $p_r(k)$, $v_r(k)$, and $a_r(k)$ represent the position, velocity, and acceleration of the virtual leading vehicle, respectively. ΔT denotes the sampling period.

The linearized discrete-time longitudinal dynamic equation for the vehicle is given by [42]

$$x_i(k+1) = A_i x_i(k) + B_i u_i(k) + C_i \omega_i(k) \tag{2}$$

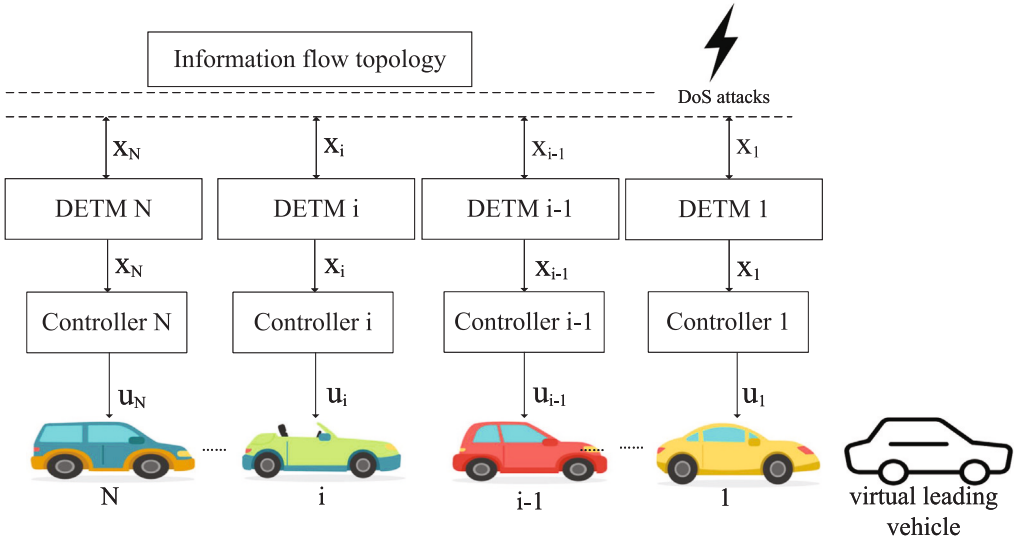


Fig. 1. System structure.

where $x_i(k) = \begin{bmatrix} p_i(k) & v_i(k) & a_i(k) \end{bmatrix}^T \in R^{3\times 1}$, $u_i(k) \in R$, and $\omega_i(k) \in R$ are the state, control input, and external disturbance of ith vehicle, respectively, $i = 1, 2, \ldots, \mathcal{N}$. In this paper, the external disturbance is assumed to be bounded, i.e., $\|\omega_i(k)\|^2 \leqslant \|W\|^2$. $p_i(k)$, $v_i(k)$ and $a_i(k)$ represent the position, velocity and acceleration of the ith vehicle, respectively. $A_i = \begin{bmatrix} 1 & \Delta T & 0 \\ 0 & 1 & \Delta T \\ 0 & 0 & 1-\frac{\Delta T}{\tau_i} \end{bmatrix}$, $B_i = \begin{bmatrix} 0 \\ 0 \\ \frac{\Delta T}{\tau_i} \end{bmatrix}$ and $C_i = \begin{bmatrix} 0 \\ 0 \\ \Delta T \end{bmatrix}$ are constant matrices. τ_i denotes the engine inertia time constant of the ith vehicle.

Remark 1. The studies of CVP system based on this linearized vehicle model have received much attention, see, e.g., [41–43]. In this paper, we will use this linearized vehicle model as the control plant, and the main goal is to design the cooperative control strategy for CVP system subject to DoS attacks and constraints.

2.3. DoS attacks

In this paper, it is assumed that DoS attacks can occur randomly on any communication channel of the CVP system, and the adversary will block the data transmission among the vehicles. Define $\{\mathcal{L}_i\}_{i\in \mathrm{N}^+}$ as the instant when the ith DoS attacks occur and n_i denote the duration of the ith DoS attacks, where $n_i > 0$. Thus, the activity time of DoS attacks in the interval $[0, k]$ can be represented as

$$\Gamma(0,k) = \bigcup_{i\in \mathrm{N}^+} [\mathcal{L}_i + n_i) \bigcap [0,k] \tag{3}$$

Define $\Gamma_{tot}(0,k)$ as the length of $\Gamma(0,k)$, and then the following assumptions are introduced to describe the DoS attacks.

Assumption 1 ([44]). For DoS attacks duration, there exist constants σ and T_a such that

$$\Gamma_{tot}(0,k) \leqslant \sigma + \frac{k}{T_a} \tag{4}$$

holds for all $k \in N^+$, where $\sigma \geqslant 0$ and $T_a \geqslant 1$.

Assumption 2 ([42]). It is assumed that $\Psi_{\max} = \sigma + \frac{k}{T_a}$ is the maximum total duration of DoS attacks in the time interval $[0, k]$, the maximum duration of a single DoS attacks is N_a.

Remark 2. The modeling of DoS attacks has been investigated in many articles [44–48]. The above two assumptions have practical significance because adversaries may need to hide their attack strategy to avoid detection, i.e., they may not launch an attack at every time instant, and the attack is also subject to power consumption, which is always limited.

2.4. Problem description

The objective of this paper is to design a resilient controller such that all vehicles can track the state of the virtual leading vehicle and the desired spacing between two contiguous vehicles in the CVP system is guaranteed, which can be represented as

$$\begin{cases} \lim_{k\to\infty} \left(p_{i-1}(k) - p_i(k) - d\right) = 0 \\ \lim_{k\to\infty} \left(v_i(k) - v_r(k)\right) = 0 \\ \lim_{k\to\infty} \left(a_i(k) - a_r(k)\right) = 0 \end{cases} \tag{5}$$

The parameters of vehicles in the CVP system are usually constrained during traveling. For instance, the constraints for speed and acceleration are usually required for driving safety and passenger comfort, and the input constraint is limited by the physical conditions of the vehicle, which can be represented as

$$\begin{cases} v_{i,\min} \leqslant v_i(k) \leqslant v_{i,\max} \\ a_{i,\min} \leqslant a_i(k) \leqslant a_{i,\max} \\ u_{i,\min} \leqslant u_i(k) \leqslant u_{i,\max} \end{cases} \tag{6}$$

where $v_{i,\min}$, $a_{i,\min}$, and $u_{i,\min}$ denote the minimum values of the velocity, acceleration, and control input, respectively. $v_{i,\max}$, $a_{i,\max}$, and $u_{i,\max}$ denote the maximum values of the velocity, acceleration, and control input, respectively. The constraints on the system state and control input can be expressed as $x_i(k) \in \mathrm{X}_i \subseteq R^{3\times 1}$ and $u_i(k) \in \mathcal{U}_i \subseteq R$.

Define the tracking error of the ith vehicle as

$$e_i(k) = \begin{bmatrix} p_i(k) - p_r(k) - d_{ir} \\ v_i(k) - v_r(k) \\ a_i(k) - a_r(k) \end{bmatrix} \tag{7}$$

where $d_{ir} = i \times d$ denotes the desired spacing between ith vehicle and the virtual leading vehicle. Thus, the tracking error equation can be written as

$$e_i(k+1) = A_i e_i(k) + B_i u_i(k) + C_i \omega_i(k) \tag{8}$$

Similar to those state and control constraints, the error constraints in the tracking error Eq. (8) can be represented as $e_i(k) \in \chi_i \subseteq R^{3\times 1}$.

The following assumption is important for the control algorithm design and stability analysis.

Assumption 3 ([49]). For the system $e_i(k+1) = A_i e_i(k) + B_i u_i(k)$, the terminal set $\mathcal{H}(\eta_i)$ is defined as $\mathcal{H}(\eta_i) = \left\{ e_i \middle| \|e_i(k)\|_{P_i}^2 \leqslant {\eta_i}^2 \right\}$. When $e_i(k) \in \mathcal{H}(\eta_i)$, for given constant $\eta_i > 0$, state weighting matrix Q_i, and control weighting matrix R_i, there exist a positive definite matrix P_i and a feedback control law K_i such that

$$\|e_i(k+1)\|_{P_i}^2 - \|e_i(k)\|_{P_i}^2 \leqslant -\|e_i(k)\|_{Q_i + K_i^T R_i K_i}^2 \tag{9}$$

holds.

Remark 3. When $e_i(k) \in \mathcal{H}(\eta_i)$, P_i can be calculated from the Riccati equation ${A_i}^T P_i A_i - P_i - {A_i}^T P_i B_i ({B_i}^T P_i B_i + R_i)^{-1} {B_i}^T P_i A_i + Q_i = 0$ and K_i can be calculated by $K_i = ({B_i}^T P_i B_i + R_i)^{-1} {B_i}^T P_i A_i$.

3. Dynamic event-triggering and distributed model predictive control

3.1. Dynamic event-triggering mechanism

Frequent inter-vehicle communication increases the communication and computation burden. Therefore, a novel DETM is designed to reduce inter-vehicle communication.

Assuming that k_i^d is the dth triggering moment of ith vehicle, the next triggering time instant of DETM is determined as

$$k_i^{d+1} = \inf\left\{ t \in N^+ | \Phi > 0 \right\} \tag{10}$$

where $\Phi = \left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm1}}^2 - \gamma_i(k_i^d + t)\phi_i$, $\Pi_{1i}\left(k_i^d + t\right) = x_i\left(k_i^d + t\right) - x_i^B\left(k_i^d + t | k_i^d\right)$, $\gamma_i(k_i^d + t) = \Pi_{2i}(k_i^d + t)\delta_{1i}(k_i^d + t) + \left(1 - \Pi_{2i}(k_i^d + t)\right)\delta_{2i}(k_i^d + t)$, $\Pi_{2i}\left(k_i^d + t\right) = tansig\left[\Pi_{3i}\left(k_i^d + t\right)\right]$, $\Pi_{3i}\left(k_i^d + t\right) = \sum_{j \in \mathbb{C}_i} \left[x_i(k_i^d + t) - {x_j}^B(k_i^d + t | k_i^d) - d_{i,j}\right]$, ϕ_i is a positive scalar, Q_{etm1} is a positive matrix. $\Pi_{1i}\left(k_i^d + t\right)$ denotes the error between the actual state and the predicted state of the ith vehicle at k_i^d. $\Pi_{3i}\left(k_i^d + t\right)$ denotes the error between the actual state of the ith vehicle and the predicted state of its neighbors at k_i^d, $d_{i,j} = \begin{bmatrix} d_{ij} & 0 & 0 \end{bmatrix}^T$. $x_i^B\left(k_i^d + t | k_i^d\right)$ and $x_j^B\left(k_i^d + t | k_i^d\right)$ are the predicted state of ith vehicle and the predicted state of the neighboring vehicles in the received data packet at the moment k_i^d, the specific form of the data packet will be elaborated in Section 3.3. $\delta_{1i}(k_i^d + t)$ and $\delta_{2i}(k_i^d + t)$ are two online update threshold parameters, which are defined as

$$\delta_{1i}(k_i^d + t + 1) = \frac{\delta_{1i}(k_i^d + t)}{1 + \varepsilon_{1i}\delta_{1i}(k_i^d + t)\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2} \tag{11a}$$

$$\delta_{2i}(k_i^d + t + 1) = \frac{\delta_{iM} + \varepsilon_{2i}\delta_{2i}(k_i^d + t)\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2}{1 + \varepsilon_{2i}\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2} \tag{11b}$$

where $\varepsilon_{1i} \geqslant 0$, $\varepsilon_{2i} \geqslant 0$ and $0 \leqslant \delta_{im} \leqslant \delta_{iM} \leqslant 1$ are some threshold parameters for offline design, Q_{etm2} is a positive matrix. The following theorem introduce the key properties of our proposed DETM condition.

Theorem 1. *Given positive scalars $\varepsilon_{1i} > 0$, $\varepsilon_{2i} > 0$, $\delta_{iM} \geqslant \delta_{im} \geqslant 0$, $0 \leqslant \delta_{1i}(0) \leqslant \delta_{im}$, $\delta_{im} \leqslant \delta_{2i}(0) \leqslant \delta_{iM}$ and positive definite matrix Q_{etm2}, the sequence $\left\{\delta_{1i}(k_i^d)\right\}$ is monotonically non-increasing and satisfies $0 \leqslant \delta_{1i}(k_i^d) \leqslant \delta_{1i}(0) \leqslant \delta_{1m}$, the sequence $\left\{\delta_{2i}(k_i^d)\right\}$ is monotonically non-decreasing and satisfies $\delta_{im} \leqslant \delta_{2i}(0) \leqslant \delta_{2i}(k_i^d) \leqslant \delta_{iM}$ and the dynamic threshold parameter $\gamma_i(k_i^d)$ satisfies $0 \leqslant \delta_{1i}(k_i^d) \leqslant \gamma_i(k_i^d) \leqslant \delta_{2i}(k_i^d) \leqslant \delta_{iM}$.*

Proof. First, we analyze the monotonicity of $\left\{\delta_{1i}(k_i^d)\right\}$ as

$$\begin{aligned}
&\delta_{1i}(k_i^d + t + 1) - \delta_{1i}(k_i^d + t) \\
&= \frac{\delta_{1i}(k_i^d + t)}{1 + \varepsilon_{1i}\delta_{1i}(k_i^d + t)\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2} - \delta_{1i}(k_i^d + t) \\
&= \frac{-{\delta_{1i}}^2(k_i^d + t)\varepsilon_{1i}\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2}{1 + \varepsilon_{1i}\delta_{1i}(k_i^d + t)\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2} \leqslant 0
\end{aligned} \tag{12}$$

It can be obtained that the sequence $\left\{\delta_{1i}(k_i^d)\right\}$ is monotonically non-decreasing and $\delta_{1i}(k_i^d) \geqslant 0$.

Then it follows from $\left\{\delta_{2i}(k_i^d)\right\}$ that

$$\begin{aligned}
&\delta_{2i}(k_i^d + t + 1) - \delta_{iM} \\
&= \frac{\delta_{iM} + \varepsilon_{2i}\delta_{2i}(k_i^d + t)\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2}{1 + \varepsilon_{2i}\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2} - \delta_{iM} \\
&= \frac{\varepsilon_{2i}\left[\delta_{2i}(k_i^d + t) - \delta_{iM}(k_i^d + t)\right]\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2}{1 + \varepsilon_{2i}\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2} \\
&\leqslant 0
\end{aligned} \tag{13}$$

which implies $\delta_{2i}(k_i^d) \leqslant \delta_{iM}$. Applying the similar derivation of (12) to the $\left\{\delta_{2i}(k_i^d)\right\}$, one can obtain that

$$\begin{aligned}
&\delta_{2i}(k_i^d + t + 1) - \delta_{2i}(k_i^d + t) \\
&= \frac{\delta_{iM} + \varepsilon_{2i}\delta_{2i}(k_i^d + t)\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2}{1 + \varepsilon_{2i}\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2} - \delta_{2i}(k_i^d + t) \\
&= \frac{\delta_{iM} - \delta_{2i}(k_i^d + t)}{1 + \varepsilon_{2i}\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2} \geqslant 0
\end{aligned} \tag{14}$$

It means that the sequence $\left\{\delta_{2i}(k_i^d)\right\}$ is monotonically non-decreasing.

As for $\gamma_i(k_i^d)$, the following inequalities hold

$$\begin{aligned}
&\gamma_i(k_i^d + t) - \delta_{1i}(k_i^d + t) \\
&\quad = \left[1 - \Pi_{2i}\left(k_i^d + t\right)\right]\left(\delta_{2i}(k_i^d + t) - \delta_{1i}(k_i^d + t)\right) \geqslant 0
\end{aligned} \tag{15}$$

$$\begin{aligned}
&\gamma_i(k_i^d + t) - \delta_{2i}(k_i^d + t) \\
&\quad = \Pi_{2i}\left(k_i^d + t\right)\left[\delta_{1i}(k_i^d + t) - \delta_{2i}(k_i^d + t)\right] \leqslant 0
\end{aligned} \tag{16}$$

It follows from (15) and (16) that $\gamma_i(k_i^d)$ satisfies $0 \leqslant \delta_{1i}(k_i^d) \leqslant \gamma_i(k_i^d) \leqslant \delta_{2i}(k_i^d) \leqslant \delta_{iM}$. This completes the proof.

Remark 4. The threshold parameters of the DETM can be dynamically adjusted by the error between the actual state of the ith vehicle and the predicted state in the buffer. The threshold parameter will decrease as the error between the actual state of the ith vehicle and the predicted state in the buffer becomes larger. It can effectively reduce the communication and computation burden. When DoS attacks occur, the error between the actual state and the predicted state of the ith vehicle will increase due to external disturbance and the inability to solve the optimization problem, and the error between the predicted state of the ith vehicle and the neighbor vehicle will also increase. In this case, the value of $\Pi_{2i}\left(k_i{}^d + t\right)$ will become larger, the value of $\delta_{1i}(k_i^d + t)$ will become smaller, and the value of $\gamma_i(k_i^d + t)$ will therefore become smaller. The ith vehicle will trigger more frequently as the threshold parameter of the DTEM becomes smaller, thus enabling the ith vehicle to achieve cooperative control with the neighbor vehicle.

3.2. Distributed model predictive control

In this section, we are on the stage to discuss the DMPC design. For each vehicle in the CVP system, we assume that the prediction horizon of the finite horizon optimization problem is N. First, the following three types of sequences are defined as

1. $\tilde{x}_i(k_i^d + t | k_i^d)$ and $\tilde{u}_i(k_i^d + t | k_i^d)$ are the predicted state sequence and the predicted control input sequence.
2. ${x_i}^*(k_i^d + t | k_i^d)$ and ${u_i}^*(k_i^d + t | k_i^d)$ are the optimal state sequence and input sequence generated under the finite horizon optimization problem at moment k_i^d. The finite horizon optimization problem are defined later in this section.

3. ${x_i}^B(k_i^d+t|k_i^d)$ and ${u_i}^B(k_i^d+t|k_i^d)$ are the optimal state sequence and optimal input sequence stored in the buffer obtained by solving the finite time domain optimization problem at moment k_i^d.

The cost function of ith vehicle is defined as

$$J_i\left(\tilde{x}_i(k_i^d),\tilde{u}_i(k_i^d),X_i^a(k_i^d)\right)=J_{i1}\left(k_i^d\right)+J_{i2}\left(k_i^d\right)+V_{iN}\left(k_i^d\right) \tag{17}$$

where $J_{i1}(k_i^d)=\sum_{n=0}^{N-1}\left[\left\|\tilde{e}_i(k_i^d+n|k_i^d)\right\|_{Q_i}^2+\left\|\tilde{u}_i(k_i^d+n|k_i^d)\right\|_{R_i}^2\right]$, $J_{i2}(k_i^d)=\sum_{n=0}^{N-1}\sum_{j\in\mathbb{C}_i}\left\|\tilde{x}_i(k_i^d+n|k_i^d)-x_j^B(k_i^d+n|k_i^d)-d_{i,j}\right\|_{Q_{ij}}^2$, $V_{iN}(k_i^d)=\left\|\tilde{e}_i(k_i^d+N|k_i^d)\right\|_{P_i}^2$, $\tilde{e}_i(k_i^d+n|k_i^d)=\tilde{x}_i(k_i^d+n|k_i^d)-x_r(k_i^d+n)-d_{i,r}$, $J_{i1}(k_i^d)$ is the cost function of the tracking error and control input, $J_{i2}(k_i^d)$ is the cost function for the state error of the ith vehicle and its neighbors, $V_{iN}(k_i^d)$ is the terminal cost function, Q_{ij} is weighting matrix, $X_i^a(k_i^d)$ denotes the total number of data packets that ith vehicle can receive at k_i^d.

We design robustness constraints to the optimization problem for each vehicle, and the finite horizon optimization problem for ith vehicle can be expressed as

$$\min J_i(\tilde{x}_i(k_i^d),\tilde{u}_i(k_i^d),X_i^a(k_i^d))$$

s.t.

$$\|\tilde{e}_i(k_i^d+n|k_i^d)\|^2\in\left(1-\frac{n}{N}\varsigma_i\right)\|\chi_i\|^2 \tag{18a}$$

$$\tilde{u}_i(k_i^d+n|k_i^d)\in\mathcal{U}_i \tag{18b}$$

$$\tilde{x}_i(k_i^d+n+1|k_i^d)=A_i\tilde{x}_i(k_i^d+n|k_i^d)+B_i\tilde{u}_i(k_i^d+n|k_i^d) \tag{18c}$$

$$\|\tilde{e}_i(k_i^d+N|k_i^d)\|_{P_i}^2\le\alpha_i^2\varepsilon_i^2 \tag{18d}$$

for $n\in[0,N-1]$

where (18a) and (18d) are tightening state constraints and tightening terminal constraints, aiming to make the tracking error of the ith vehicle tighter. $\varsigma_i\in(0,1)$ and $\alpha_i\in(0,1)$ are robust constraint parameters. (18b) is the input constraint of the ith vehicle. The finite horizon optimization problem is established to minimize the cost function and the input to the system subject to the input constraints.

Remark 5. It is noted that the leading vehicle only needs to follow the state of the virtual leading vehicle. Thus, we assume that the leading vehicle can always carry out the finite horizon optimization problem to improve the operation efficiency in the CVP system.

Remark 6. The robustness constraint ensures that the system tracking error sequence has an upper bound on the decreasing function even in the external disturbance. The coordination of the entire CVP system is achieved by minimizing the cost function through a finite horizon optimization problem for each vehicle.

3.3. Buffer and data packet design

Due to the existence of DoS attacks and DETM, it is necessary to design the format of buffer and data packet. Since the condition of the event-triggering is related to the state information transmitted by its vehicle and the neighboring vehicles at the moment of triggering, this information should be stored in the form of data packets in the buffer. Considering the existence of DoS attacks, we use a lengthened sequence of state and control inputs in the data packet. The input sequence in the data packet is

$${U_i}^B(k_i^d+n|k_i^d)=\begin{cases}{u_i}^*(k_i^d+n|k_i^d), & n\in[0,N-1]\\ K_ie_i(k_i^d+n|k_i^d), & n\in\left[N,N+N_a-1\right]\end{cases} \tag{19}$$

For $n\in\left[0,N+N_a-1\right]$, the sequence of state in the data packet is

$${X_i}^B(k_i^d+n+1|k_i^d)=A{x_i}^*(k_i^d+n|k_i^d)+B{U_i}^B(k_i^d+n|k_i^d) \tag{20}$$

Since the event-triggering instant of each vehicle cannot be synchronized, thus the transmitted data is not necessarily the optimal state sequence and the optimal input sequence of the neighboring vehicles at the triggering moment. To ensure that the amount of data in the packet transmitted to the neighboring vehicles is more than or equal to N, we design the format of the data packet. Before the next triggering instant, the first data in the data packet is deleted in every sampling period, and the state and input data obtained through state feedback are added at the end. The real-time updating of data packets is an excellent way to ensure the integrity and validity of the transmitted data.

4. Main results

In this section, the recursive feasibility of the DETM-based DMPC algorithm proposed in this paper and the stability of the CVP system under DoS attacks are analyzed. The following definition is significant for the analysis of stability:

Definition 1 (*[50]*)**.** Considering the system (8), the external disturbance satisfies $\|\omega_i(k)\|^2\le\|W\|^2$, if there exists a function $V\left(e_i(k)\right)$, $\mathcal{K}_\infty$ class functions α_1, α_2, and ρ_1, a $\mathcal{K}$ class function ρ_2, constants $\beta_1\ge0$ and $\beta_2\ge0$ such that

$$\alpha_1(\|e_i(k)\|)\leqslant V(e_i(k))\leqslant\alpha_2(\|e_i(k)\|)+\beta_1 \tag{21}$$

$$V(e_i(k+1))-V(e_i(k))\leqslant-\rho_1(\|e_i(k)\|)+\rho_2(\|W\|)+\beta_2 \tag{22}$$

hold. Then the system (8) is input-to-state practical stability (ISPS).

4.1. Recursive feasibility analysis

It is assumed that the DETM-based DMPC algorithm proposed in the previous section is initially feasible. Recursive feasibility means that the finite horizon optimization problem in Section 3.2 is feasible at each triggering moment.

Theorem 2. *On the basis of DETM (10), the finite horizon optimization problem (18) is recursively feasible at the triggering moment k_i^d if the following conditions are satisfied:*

$$\theta_i\le\left(\frac{1}{N\left[\lambda_{\max}({A_i}^TA_i)\right]^{N-1}}\zeta_i\right)\|\chi_i\|^2, \tag{23}$$

$$\theta_i\le\frac{(1-{\alpha_i}^2){\eta_i}^2}{\lambda_{\max}(P_i)\left[\lambda_{\max}({A_i}^TA_i)\right]^{N-1}}, \tag{24}$$

$$\theta_i\le\frac{(1-{\alpha_i}^2){\eta_i}^2}{\lambda_{\max}(P_i)}, \tag{25}$$

$$\alpha_i\ge\sqrt{\frac{\lambda_{\max}\left(P_i\right)}{\lambda_{\min}\left(Q_i+{K_i}^TR_iK_i\right)+\lambda_{\max}\left(P_i\right)}}, \tag{26}$$

$$\alpha_i\ge\sqrt{\frac{\lambda_{\max}(P_i)}{N\lambda_{\min}(Q_i+{K_i}^TRK_i)+\lambda_{\max}(P_i)}}. \tag{27}$$

where

$$\theta_i=\theta_{i1}+\theta_{i2},$$

$$\theta_{i1}=\left[\lambda_{\max}\left({A_i}^TA_i\right)\right]^{N_a+1}\frac{\delta_{iM}\phi_i}{\lambda_{\min}\left(Q_{etm1}\right)},$$

$$\theta_{i2}=\frac{1-\left[\lambda_{\max}\left({A_i}^TA_i\right)\right]^{N_a}}{1-\lambda_{\max}\left({A_i}^TA_i\right)}\lambda_{\max}\left({C_i}^TC_i\right)\|W\|^2.$$

Proof. It is assumed that k_i^d is the current triggering moment and $\bar{k}_i^{d+1}$ is the next triggering time instant that satisfies the event-triggering condition (10). Then we can get

$$\left\|x_i\left(\bar{k}_i^{d+1}-1\right)-x_i^B\left(\bar{k}_i^{d+1}-1|k_i^d\right)\right\|_{Q_{etm1}}^2\le\delta_{iM}\phi_i \tag{28}$$

which implies

$$\left\| x_i\left(\bar{k}_i^{d+1}-1\right)-x_i^B\left(\bar{k}_i^{d+1}-1|k_i^d\right)\right\|^2 \le \frac{\delta_{iM}\phi_i}{\lambda_{\min}\left(Q_{etm1}\right)} \tag{29}$$

Next, consider the worst-case scenario where the ith vehicle suffers DoS attacks of maximum duration N_a at $\bar{k}_i^{d+1}$. The next triggering time instant in the worst-case scenario should be k_i^{d+1}, where $k_i^{d+1}=\bar{k}_i^{d+1}+N_a$. Thus, the error between the actual state and the predicted state of the ith vehicle in the worst-case scenario is

$$\begin{aligned} &x_i(k_i^{d+1})-x_i{}^*(k_i^{d+1}|k_i^d)\\ &\quad=x_i(\bar{k}_i^{d+1}+N_a)-x_i{}^*(\bar{k}_i^{d+1}+N_a|k_i^d)\\ &\quad=A_i{}^{N_a+1}\left[x_i(\bar{k}_i^{d+1}-1)-x_i{}^*(\bar{k}_i^{d+1}-1|k_i^d)\right]\\ &\qquad+A_i{}^{N_a}C_i\omega_i(\bar{k}_i^{d+1}-1)+\cdots+C_i\omega_i(\bar{k}_i^{d+1}+N_a-1) \end{aligned} \tag{30}$$

Thus, one can obtain that

$$\begin{aligned} \left\|x_i(k_i^{d+1})-x_i{}^*(k_i^{d+1}|k_i^d)\right\|^2 \le&\left[\lambda_{\max}\left(A_i{}^TA_i\right)\right]^{N_a+1}\frac{\delta_{iM}\phi_i}{\lambda_{\min}\left(Q_{etm1}\right)}\\ &+\sum_{m=0}^{N_a}\left(\|A_i\|^2\right)^m\|C_i\omega_i\|^2\\ \le&\theta_i \end{aligned} \tag{31}$$

The above θ_i is the upper bound on the error between the actual state and the predicted state at the next triggering instant. To ensure the recursive feasibility, it is essentially sufficient to show that the candidate state sequence generated by the candidate control input sequence at triggering moment k_i^{d+1} is feasible. Next, we discuss the two cases of k_i^{d+1}.

Case 1: $k_i^{d+1}\in\left(k_i^d,k_i^d+N\right]$

The error between the candidate state and predicted state can be written as

$$\bar{x}_i(k_i^{d+1}+t|k_i^{d+1})-x_i{}^*(k_i^{d+1}+t|k_i^d)=A_i{}^t\left[x_i(k_i^{d+1})-x_i{}^*(k_i^{d+1}|k_i^d)\right] \tag{32}$$

one can obtain that

$$\begin{aligned} &\left\|\bar{x}_i(k_i^{d+1}+t|k_i^{d+1})-x_i{}^*(k_i^{d+1}+t|k_i^d)\right\|^2\\ &\quad=\left\|\bar{e}_i(k_i^{d+1}+t|k_i^{d+1})-e_i{}^*(k_i^{d+1}+t|k_i^d)\right\|^2\\ &\quad\le\left[\lambda_{\max}(A_i{}^TA_i)\right]^t\left\|x_i(k_i^{d+1})-x_i{}^*(k_i^{d+1}|k_i^d)\right\|^2\\ &\quad\le\left[\lambda_{\max}(A_i{}^TA_i)\right]^t\theta_i \end{aligned} \tag{33}$$

By using the triangle inequality, it yields

$$\left\|\bar{e}_i(k_i^{d+1}+t|k_i^{d+1})\right\|^2\le\left\|e_i{}^*(k_i^{d+1}+t|k_i^d)\right\|^2+\left[\lambda_{\max}(A_i{}^TA_i)\right]^t\theta_i \tag{34}$$

When $t\in\left[0,N+k_i^d-k_i^{d+1}\right]$, due to the fact that θ_i satisfies condition (23), it can be obtained that

$$\begin{aligned} &\left\|\bar{e}_i(k_i^{d+1}+t|k_i^{d+1})\right\|^2\\ &\quad\le\left\|e_i{}^*(k_i^{d+1}+t|k_i^d)\right\|^2+\left[\lambda_{\max}(A_i{}^TA_i)\right]^t\theta_i\\ &\quad\le\left(1-\frac{k_i^{d+1}+t-k_i^d}{N}\zeta_i\right)\|\chi_i\|^2+\left[\lambda_{\max}(A_i{}^TA_i)\right]^t\theta_i\\ &\quad\le\left(1-\frac{t}{N}\zeta_i\right)\|\chi_i\|^2 \end{aligned} \tag{35}$$

Applying the similar derivation of (33), it leads to

$$\begin{aligned} &\left\|\bar{e}_i(k_i^d+N|k_i^{d+1})-e_i{}^*(k_i^d+N|k_i^d)\right\|^2\\ &\quad\le\left[\lambda_{\max}(A_i{}^TA_i)\right]^{k_i^d+N-k_i^{d+1}}\theta_i\\ &\quad\le\left[\lambda_{\max}(A_i{}^TA_i)\right]^{N-1}\theta_i \end{aligned} \tag{36}$$

By adopting matrix transformation scheme and triangle inequality, one has

$$\begin{aligned} &\left\|\bar{e}_i(k_i^d+N|k_i^{d+1})\right\|_{P_i}^2\\ &\quad\le\left\|e_i{}^*(k_i^d+N|k_i^d)\right\|_{P_i}^2+\lambda_{\max}(P_i)\left[\lambda_{\max}(A_i{}^TA_i)\right]^{N-1}\theta_i \end{aligned} \tag{37}$$

Since θ_i satisfies condition (24), the inequality (37) can be written as

$$\left\|\bar{e}_i(k_i^d+N|k_i^{d+1})\right\|_{P_i}^2\le\alpha_i{}^2\eta_i^2+(1-\alpha_i{}^2)\eta_i^2=\eta_i^2 \tag{38}$$

which implies $\left\|\bar{e}_i(k_i^d+N|k_i^{d+1})\right\|_{P_i}^2\le\eta_i{}^2$.

When $t\in\left[0,k_i^{d+1}-k_i^d\right)$, it follows from Assumption 3, we have

$$\begin{aligned} &\left\|\bar{e}_i(k_i^d+t+1+N|k_i^{d+1})\right\|_{P_i}^2-\left\|\bar{e}_i(k_i^d+t+N|k_i^{d+1})\right\|_{P_i}^2\\ &\quad\le-\left\|\bar{e}_i(k_i^d+t+N|k_i^{d+1})\right\|_{Q_i+K_i{}^TR_iK_i}^2 \end{aligned} \tag{39}$$

Summing the left and right sides of inequality (39) from $t=0$ to $t=k_i^{d+1}-k_i^d-1$, respectively, it yields

$$\left\|\bar{e}_i(k_i^{d+1}+N|k_i^{d+1})\right\|_{P_i}^2\le\frac{\lambda_{\max}(P_i)}{\lambda_{\min}(Q_i+K_i{}^TR_iK_i)+\lambda_{\max}(P_i)}\eta_i{}^2 \tag{40}$$

Based on the condition (26), one has

$$\left\|\bar{e}_i(k_i^{d+1}+N|k_i^{d+1})\right\|_{P_i}^2\le\alpha_i{}^2\eta_i^2 \tag{41}$$

Case 2: $k_i^{d+1}\in\left(k_i^d+N,k_i^d+N+N_a\right]$

The tracking error at the moment k_i^{d+1} satisfies the terminal constraint

$$\left\|e_i(k_i^{d+1})\right\|_{P_i}^2\le\left\|e_i{}^*(k_i^{d+1}|k_i^d)\right\|_{P_i}^2+\lambda_{\max}(P_i)\theta_i \tag{42}$$

Since θ_i satisfies condition (25), the inequality (42) can be written as

$$\left\|e_i(k_i^{d+1})\right\|_{P_i}^2\le\eta_i{}^2 \tag{43}$$

When $t\in[0,N-1)$, we have

$$\begin{aligned} &\left\|\bar{e}_i(k_i^{d+1}+t+1|k_i^{d+1})\right\|_{P_i}^2-\left\|\bar{e}_i(k_i^{d+1}+t|k_i^{d+1})\right\|_{P_i}^2\\ &\quad\le-\left\|\bar{e}_i(k_i^{d+1}+t|k_i^{d+1})\right\|_{Q_i+K_i{}^TR_iK_i}^2 \end{aligned} \tag{44}$$

Summing the left and right sides of inequality (44) from $t=0$ to $t=N-1$, respectively, it yields

$$\left\|\bar{e}_i(k_i^{d+1}+N|k_i^{d+1})\right\|_{P_i}^2-\left\|e_i(k_i^{d+1})\right\|_{P_i}^2\le-N\left\|\bar{e}_i(k_i^{d+1}+N|k_i^{d+1})\right\|_{Q_i+K_i{}^TR_iK_i}^2 \tag{45}$$

By adopting matrix transformation scheme, we have

$$\left\|\bar{e}_i(k_i^{d+1}+N|k_i^{d+1})\right\|_{P_i}^2\le\eta_i{}^2\frac{\lambda_{\max}(P_i)}{N\lambda_{\min}(Q_i+K_i{}^TRK_i)+\lambda_{\max}(P_i)} \tag{46}$$

According to the condition (27), one has

$$\left\|\bar{e}_i(k_i^{d+1}+N|k_i^{d+1})\right\|_{P_i}^2\le\alpha_i{}^2\eta_i{}^2 \tag{47}$$

From the above analysis, it can be demonstrated that the holding of conditions (23), (24), (25), (26), and (27) can ensure the recursive feasibility of the DETM-based DMPC algorithm proposed in this paper. This completes the proof.

4.2. Stability analysis

In this section, we are on the stage to investigate the stability of system (8) under DoS attacks.

Theorem 3. *The system (8) subjected to DoS attacks under our proposed DETM-based DMPC algorithm is ISPS if Theorem 2 holds.*

Proof. Selecting the optimal cost function at the triggering moment as the ISPS-Lyapunov function, so the ISPS-Lyapunov function for consecutive triggering moment can be expressed as $V_i^*(k_i^d) = J_i(x_i^*(k_i^d), u_i^*(k_i^d), X_i^a(k_i^d))$ and $V_i^*(k_i^{d+1}) = J_i(x_i^*(k_i^{d+1}), u_i^*(k_i^{d+1}), X_i^a(k_i^{d+1}))$. To facilitate the analysis of stability, define the candidate cost function obtained through the candidate state sequence and the candidate input sequence at moment k_i^{d+1} as $\bar{V}_i(k_i^{d+1}) = J_i(\bar{x}_i(k_i^{d+1}), \bar{u}_i(k_i^{d+1}), X_i^a(k_i^{d+1}))$. Considering that $V_i^*(k_i^{d+1})$ is the optimal cost function at moment k_i^{d+1}, it can be obtained that

$$V_i^*(k_i^{d+1}) - V_i^*(k_i^d) \leqslant \bar{V}_i(k_i^{d+1}) - V_i^*(k_i^d) \tag{48}$$

Define $\hat{V}_i(k_i^{d+1})$ as

$$\begin{aligned}\hat{V}_i(k_i^{d+1}) = &\sum_{t=0}^{N-1}\left[E_1(t) + \left\|u_i^*(k_i^{d+1}+t|k_i^d)\right\|_{R_i}^2\right] \\ &+ \sum_{t=0}^{N-1} E_2(t) + \left\|e_i^*(k_i^{d+1}+N|k_i^d)\right\|_{P_i}^2\end{aligned} \tag{49}$$

where

$$E_1(t) = \left\|x_i^*(k_i^{d+1}+t|k_i^d) - x_r(k_i^{d+1}+t) - d_{ir}\right\|_{Q_i}^2,$$

$$E_2(t) = \sum_{j\in\mathbb{C}_i}\left\|x_i^*(k_i^{d+1}+t|k_i^d) - x_j{}^B(k_i^{d+1}+t|k_i^d) - d_{ij}\right\|_{Q_{ij}}^2.$$

By subtracting and adding $\hat{V}_i(k_i^{d+1})$ in (48), one can obtain that

$$V_i^*(k_i^{d+1}) - V_i^*(k_i^d) \leqslant \bar{V}_i(k_i^{d+1}) - \hat{V}_i(k_i^{d+1}) + \hat{V}_i(k_i^{d+1}) - V_i^*(k_i^d) \tag{50}$$

Firstly, it follows from the first term $\bar{V}_i(k_i^{d+1}) - \hat{V}_i(k_i^{d+1})$ in inequality (50) that

$$\begin{aligned}\bar{V}_i(k_i^{d+1}) - \hat{V}_i(k_i^{d+1}) \leqslant &\sum_{t=0}^{N-1}\left[E_3(t) + E_4(t) + E_5(t)\right] \\ &+ \left\|\bar{x}_i(k_i^{d+1}+N|k_i^{d+1}) - x_i^*(k_i^{d+1}+N|k_i^d)\right\|_{P_i}^2\end{aligned} \tag{51}$$

where

$$E_3(t) = \left\|\bar{x}_i(k_i^{d+1}+t|k_i^{d+1}) - x_i^*(k_i^{d+1}+t|k_i^d)\right\|_{Q_i}^2,$$

$$E_4(t) = \sum_{j\in\mathbb{C}_i}\left\|\bar{x}_i(k_i^{d+1}+t|k_i^{d+1}) - x_i^*(k_i^{d+1}+t|k_i^d)\right\|_{Q_{ij}}^2,$$

$$E_5(t) = \sum_{j\in\mathbb{C}_i}\left\|x_j{}^B(k_i^{d+1}+t|k_i^{d+1}) - x_j{}^B(k_i^{d+1}+t|k_i^d)\right\|_{Q_{ij}}^2.$$

From (33), we have

$$\begin{aligned}&\left\|\bar{x}_i(k_i^{d+1}+t|k_i^{d+1}) - x_i^*(k_i^{d+1}+t|k_i^d)\right\|_{Q_i}^2 \\ &\quad\leqslant \lambda_{\max}(Q_i)\left[\lambda_{\max}(A_i{}^TA_i)\right]^t\theta_i\end{aligned} \tag{52}$$

Applying the similar derivation to the other terms in (51), one can obtain that

$$\begin{aligned}\bar{V}_i(k_i^{d+1}) - \hat{V}_i(k_i^{d+1}) \leqslant &\sum_{t=0}^{N-1}\lambda_{\max}(Q_i)\left[\lambda_{\max}(A_i{}^TA_i)\right]^t\theta_i \\ &+ \sum_{t=0}^{N-1}\lambda_{\max}(P_i)\left[\lambda_{\max}(A_i{}^TA_i)\right]^N\theta_i \\ &+ \sum_{t=0}^{N-1}\sum_{j\in\mathbb{C}_i}\left[\lambda_{\max}(Q_{ij})\left[\lambda_{\max}(A_i{}^TA_i)\right]^t\theta_i\right] \\ &+ \sum_{t=0}^{N-1}\sum_{j\in\mathbb{C}_i}\left[\lambda_{\max}(Q_{ij})\left[\lambda_{\max}(A_j{}^TA_j)\right]^t\theta_j\right] \\ \leqslant &(M_1+M_2+M_3)\theta_i + M_4\end{aligned} \tag{53}$$

where

$$M_1 = \frac{\lambda_{\max}(Q_i)\left[1-\left(\lambda_{\max}(A_i{}^TA_i)\right)^{N-1}\right]}{1-\lambda_{\max}(A_i{}^TA_i)},$$

$$M_2 = \lambda_{\max}(P_i)\left[\lambda_{\max}(A_i{}^TA_i)\right]^N,$$

$$M_3 = \sum_{j\in\mathbb{C}_i}\frac{\lambda_{\max}(Q_{ij})\left[1-\left(\lambda_{\max}(A_i{}^TA_i)\right)^{N-1}\right]}{1-\lambda_{\max}(A_i{}^TA_i)},$$

$$M_4 = \sum_{j\in\mathbb{C}_i}\frac{\lambda_{\max}(Q_{ij})\left[1-\left(\lambda_{\max}(A_j{}^TA_j)\right)^{N-1}\right]}{1-\lambda_{\max}(A_j{}^TA_j)}\theta_j.$$

Then it follows from the second term $\hat{V}_i(k_i^{d+1}) - V_i^*(k_i^d)$ in the right side of inequality (50) that

Case 1: $k_i^{d+1} \in \left(k_i^d, k_i^d + N\right]$

$$\begin{aligned}\hat{V}_i(k_i^{d+1}) - V_i^*(k_i^d) = &\sum_{t=k_i^d+N}^{k_i^{d+1}+N-1}\left[E_1(t|k_i^d) + \left\|u_i^*(t|k_i^d)\right\|_{R_i}^2 + E_2(t|k_i^d)\right] \\ &- \sum_{t=k_i^d}^{k_i^{d+1}-1}\left[E_1(t|k_i^d) + \left\|u_i^*(t|k_i^d)\right\|_{R_i}^2 + E_2(t|k_i^d)\right] \\ &+ \left\|e_i^*(k_i^{d+1}+N|k_i^d)\right\|_{P_i}^2 - \left\|e_i^*(k_i^d+N|k_i^d)\right\|_{P_i}^2\end{aligned} \tag{54}$$

Furthermore, we have

$$\begin{aligned}&\left\|e_i^*(k_i^{d+1}+N|k_i^d)\right\|_{P_i}^2 - \left\|e_i^*(k_i^d+N|k_i^d)\right\|_{P_i}^2 \\ &\quad\leqslant -\sum_{t=k_i^d+N}^{k_i^{d+1}+N-1}\left[\left\|e_i^*(t|k_i^d)\right\|_{Q_i}^2 + \left\|u_i^*(t|k_i^d)\right\|_{R_i}^2\right]\end{aligned} \tag{55}$$

By substituting (55) into (54), one gets

$$\begin{aligned}\hat{V}_i(k_i^{d+1}) - V_i^*(k_i^d) &\leqslant \sum_{t=k_i^d+N}^{k_i^{d+1}+N-1}\left[E_2(t)\right] - \left\|e_i(k_i^d)\right\|_{Q_i}^2 \\ &\leqslant -\lambda_{\min}(Q_i)\left\|e_i(k_i^d)\right\|^2 + M_5\end{aligned} \tag{56}$$

where $M_5 = N\sum_{j\in\mathbb{C}_i}\left[\frac{\lambda_{\max}(Q_{ij})}{\lambda_{\min}(P_i)}\alpha_i^2\eta_i^2 + \frac{\lambda_{\max}(Q_{ij})}{\lambda_{\min}(P_j)}\alpha_j^2\eta_j^2\right]$.

Case 2: $k_i^{d+1} \in \left(k_i^d + N, k_i^d + N + N_a\right]$

Applying the similar derivation in case 1, one can obtain that

$$\begin{aligned}\hat{V}_i(k_i^{d+1}) - V_i^*(k_i^d) = &\sum_{t=0}^{N-1}E_2(t) - \sum_{t=k_i^d-k_i^{d+1}}^{k_i^d-k_i^{d+1}+N-1}E_2(t) - \sum_{t=k_i^d-k_i^{d+1}+N}^{-1}E_2(t) \\ &- \sum_{t=0}^{N-1}\left[\left\|e_i^*(k_i^d+t|k_i^d)\right\|_{Q_i}^2 + \left\|u_i^*(k_i^d+t|k_i^d)\right\|_{R_i}^2\right] \\ &- \sum_{t=k_i^d+N}^{k_i^{d+1}-1}\left[\left\|e_i^*(t|k_i^d)\right\|_{Q_i}^2 + \left\|u_i^*(t|k_i^d)\right\|_{R_i}^2\right] \\ \leqslant &-\lambda_{\min}(Q_i)\left\|e_i(k_i^d)\right\|^2 + M_5\end{aligned} \tag{57}$$

Combining the inequalities (53), (56) and (57) yields

$$V_i^*(k_i^{d+1}) - V_i^*(k_i^d) \leqslant -\lambda_{\min}(Q_i)\left\|e_i(k_i^d)\right\|^2 + a\|W\|^2 + c \tag{58}$$

where

$$a = (M_1+M_2+M_3)M_7 + M_8,$$

$$c = (M_1+M_2+M_3)M_6 + M_9 + M_5,$$

$$M_6 = \left[\lambda_{\max}\left(A_i{}^TA_i\right)\right]^{N_a+1}\frac{\delta_{iM}\phi_i}{\lambda_{\min}\left(Q_{etm1}\right)},$$

$$M_7 = \frac{1-\left[\lambda_{\max}\left(A_i{}^TA_i\right)\right]^{N_a}}{1-\lambda_{\max}\left(A_i{}^TA_i\right)}\lambda_{\max}\left(C_i{}^TC_i\right),$$

$$M_8 = \sum_{j\in\mathbb{C}_i}\left[\frac{\lambda_{\max}(Q_{ij})\left[1-\left(\lambda_{\max}(A_j{}^TA_j)\right)^{N-1}\right]}{1-\lambda_{\max}(A_j{}^TA_j)}M_{8j}\right],$$

$$M_{8j} = \frac{1-\left[\lambda_{\max}\left(A_j{}^TA_j\right)\right]^{N_a}}{1-\lambda_{\max}\left(A_j{}^TA_j\right)}\lambda_{\max}\left(C_j{}^TC_j\right),$$

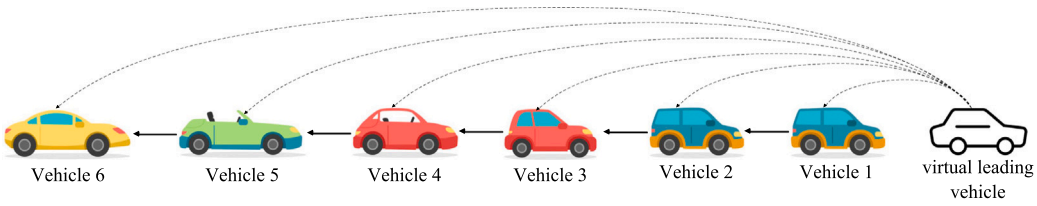
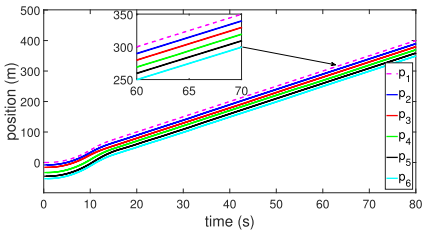
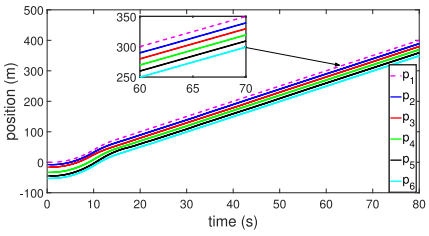


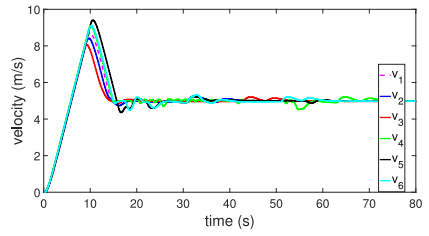
Fig. 2. Network topology.



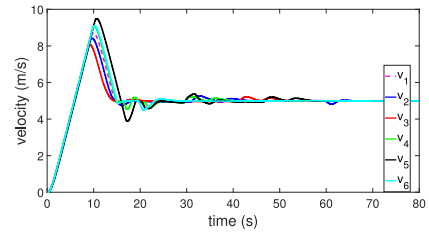
(a) Position trajectories, $\Psi_{\max} = 67$.



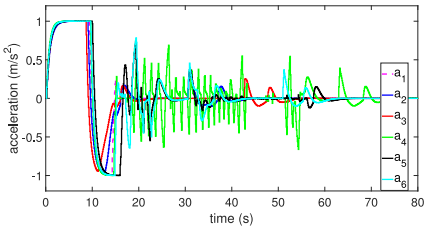
(b) Position trajectories, $\Psi_{\max} = 178$.



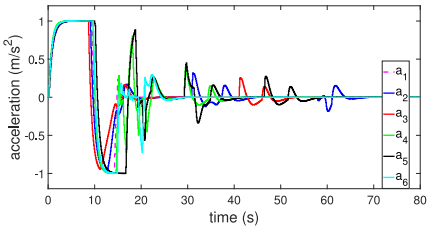
(c) Velocity trajectories, $\Psi_{\max} = 67$.



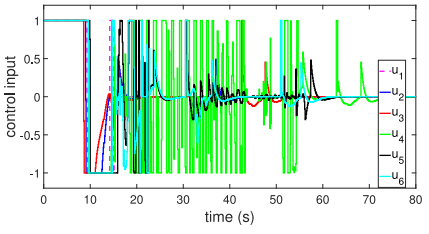
(d) Velocity trajectories, $\Psi_{\max} = 178$.



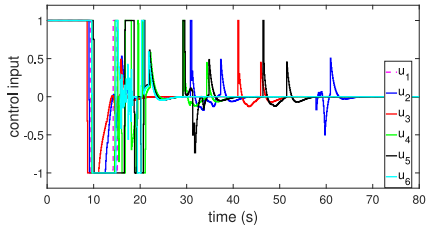
(e) Acceleration trajectories, $\Psi_{\max} = 67$.



(f) Acceleration trajectories, $\Psi_{\max} = 178$.



(g) Control input trajectories, $\Psi_{\max} = 67$.



(h) Control input trajectories, $\Psi_{\max} = 178$.

Fig. 3. The trajectories of states and control inputs.

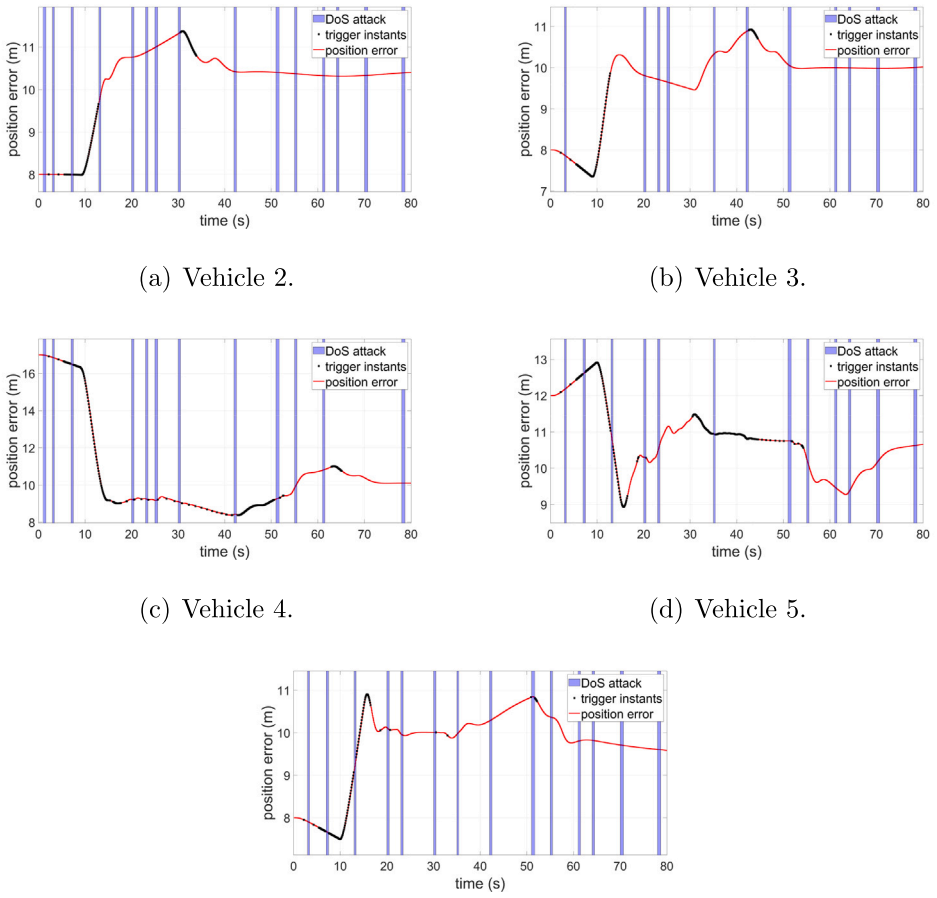
$$M_9 = \sum_{j\in\mathbb{C}_i}\left[\frac{\lambda_{\max}(Q_{ij})\left[1-\left(\lambda_{\max}(A_j{}^TA_j)\right)^{N-1}\right]}{1-\lambda_{\max}(A_j{}^TA_j)}M_{9j}\right],$$

$$M_{9j} = \left[\lambda_{\max}\left(A_j{}^TA_j\right)\right]^{N_a+1}\frac{\delta_{jM}\phi_j}{\lambda_{\min}\left(Q_{etm1}\right)}.$$

From Definition 1 and inequality (58), it can be obtained that the closed-loop system (8) is ISPS. The proof is completed.

5. Simulation

In this section, the main results of this paper are illustrated using numerical simulations performed via MATLAB.



(a) Vehicle 2. (b) Vehicle 3.

(c) Vehicle 4. (d) Vehicle 5.

(e) Vehicle 6.

Fig. 4. The position error trajectories under DoS attacks when $\Psi_{\max} = 67$.

Table 1
Vehicle Parameters.

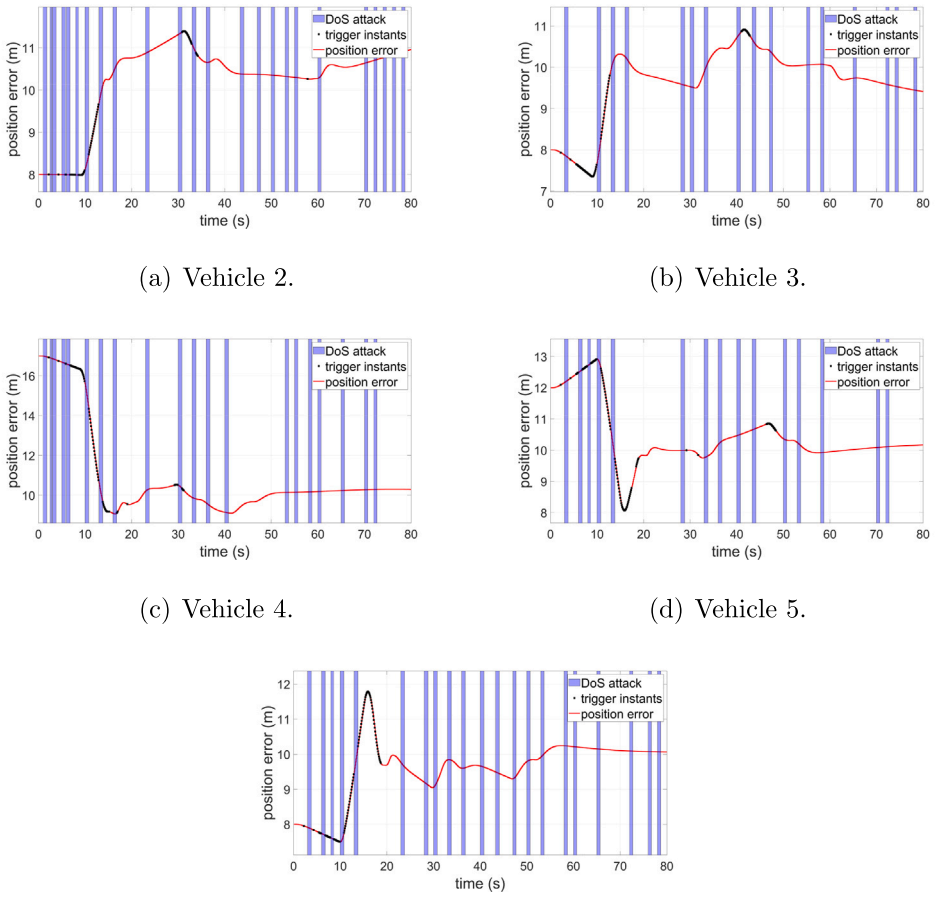
Vehicle	τ_i	$\omega_i(k)$	K_i
Vehicle 1	0.83	$0.008\sin(0.17k)$	$[-0.91 \quad -2.34 \quad -1.42]$
Vehicle 2	0.83	$0.008\sin(0.17k)$	$[-0.91 \quad -2.34 \quad -1.42]$
Vehicle 3	0.74	$0.009\sin(0.16k)$	$[-0.91 \quad -2.29 \quad -1.31]$
Vehicle 4	0.65	$0.006\sin(0.17k)$	$[-0.91 \quad -2.24 \quad -1.20]$
Vehicle 5	0.76	$0.007\sin(0.18k)$	$[-0.91 \quad -2.30 \quad -1.33]$
Vehicle 6	0.70	$0.008\sin(0.17k)$	$[-0.91 \quad -2.27 \quad -1.26]$

5.1. Parameter configuration

It is assumed that the CVP system has a virtual leading vehicle, a leading vehicle, and five following vehicles. The communication topology among the vehicles is shown in Fig. 2. The sampling period is set as $\Delta T = 0.1s$. For the DoS attacks parameters, we set $N_a = 7$. The longitudinal dynamics parameters of vehicle are choose as in [42]. In this paper, the external disturbance is assumed to be bounded, and a sinusoidal function is introduced to model the external disturbance. The engine inertia time constant, external disturbance and state feedback law for each vehicle are shown in Table 1. For the ith vehicle in the CVP system, the corresponding matrix P_i can be obtained by computing the discrete Riccati equation in Remark 3. We choose the parameters $\varsigma_i = 0.9$, $\alpha_i{}^2 = 0.99$, $\eta_i{}^2 = 9.6$, $\delta_{iM} = 2$, $\delta_{im} = 0.5$, and $\phi_i = 0.0022$. The weighting matrices are set as $Q_i = I$, $Q_{ij} = I$, $Q_{etm1} = 0.01I$, and $Q_{etm2} = I$. Considering the security and passenger comfort, the constraints imposed on each vehicle are set as $-1 \leqslant u_i \leqslant 1$, $0(\mathrm{m/s}) \leqslant v_i \leqslant 15(\mathrm{m/s})$, and $-3.5(\mathrm{m/s^2}) \leqslant a_i \leqslant 3.5(\mathrm{m/s^2})$. Assuming that the virtual leading vehicle has an initial position of 0 and travels at a constant speed of 5 m/s, the ideal vehicle spacing is $d = 10$ m. The initial state of each vehicle is set to $x_1(0) = [0;0;0]$, $x_2(0) = [-8;0;0]$, $x_3(0) = [-16;0;0]$, $x_4(0) = [-33;0;0]$, $x_5(0) = [-45;0;0]$, and $x_6(0) = [-53;0;0]$, respectively.

5.2. Platoon control under different DoS attacks durations

In order to verify the effectiveness of the proposed algorithm, the control of CVP system under different DoS attacks durations is simulated. In simulation, the DoS attacks durations are set to be $\Psi_{\max} = 67$ and $\Psi_{\max} = 178$, respectively. The state trajectories of each vehicle when $\Psi_{\max} = 67$ and $\Psi_{\max} = 178$ are shown in Fig. 3. Under two different DoS attack durations, it can be seen that all vehicles can reach the desired spacing, and achieve the same speed and acceleration as the virtual leader vehicle. The control inputs for all vehicles satisfy the input constraints. For the 2-nd to 6-th following vehicle, the position error $\Delta p_i(k)$ is defined as $\Delta p_i(k) = p_{i-1}(k) - p_i(k), i \in [2,6]$. The position error, DoS attacks sequence and event-triggering sequence for each vehicle when $\Psi_{\max} = 67$ and $\Psi_{\max} = 178$ are shown in Fig. 4 and Fig. 5, respectively. We can see that the DETM can handle DoS attacks by reducing transmission frequency. The simulation results show that the proposed DETM-based DMPC algorithm can effectively deal with the cooperative control of CVP system under different DoS attack durations.



(a) Vehicle 2. (b) Vehicle 3.

(c) Vehicle 4. (d) Vehicle 5.

(e) Vehicle 6.

Fig. 5. The position error trajectories under DoS attacks when $\Psi_{\max} = 178$.

5.3. Platoon control under different control algorithms

In order to better demonstrate the performance of algorithm proposed in this paper, we compare it with the algorithm in [42] under the same DoS attacks sequence when $\Psi_{\max} = 67$. The evaluation method in [41] is used to quantitatively assess the effectiveness of the proposed algorithm in terms of resilient control performance and communication scheduling. First, the average triggering rate F_{ave} in the time interval $[0, T_{end}]$ is defined as

$$F_{ave} = \frac{1}{\mathcal{N}-1}\sum_{i=2}^{\mathcal{N}}\left(\frac{1}{T_{end}}\sum_{k=0}^{T_{end}}\mathcal{O}_{ik}\right)\cdot 100\%$$

where

$$\mathcal{O}_{ik} = \begin{cases} 1, & \text{DTEM condition is satisfied at instant } k \\ 0, & \text{otherwise} \end{cases}$$

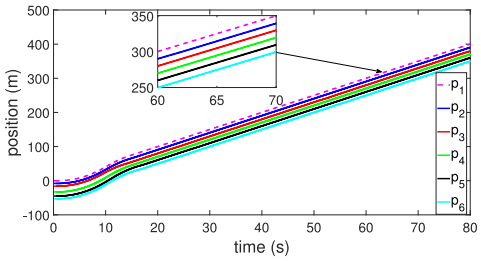
Then, the average position error e_{ave} in the time interval $[0, T_{end}]$ is defined as

$$e_{ave} = \frac{1}{\mathcal{N}-1}\sum_{i=2}^{\mathcal{N}}\left(\frac{1}{T_{end}}\sum_{k=0}^{T_{end}} p_{i-1}(k) - p_i(k) - d\right)$$

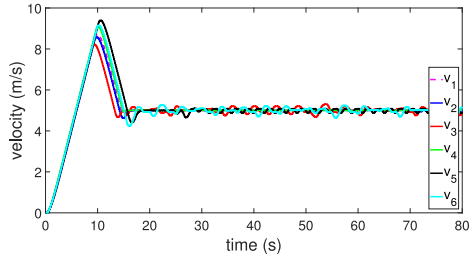
By calculating the data in the simulation, the average triggering rate and the average position error under our proposed algorithm are calculated as $F_{ave} = 0.206$ and $e_{ave} = 0.876$. The state trajectories and control input trajectories of the comparison simulation are shown in Fig. 6. The average triggering rate and the average position error in the comparison simulation are calculated as $F_{ave} = 0.386$ and $e_{ave} = 0.805$. It can be obtained that the comparison simulation have a lower average position error rate and a more significant average triggering rate. Our proposed algorithm reduces the number of triggers by 46.6% in the time interval $[0, 800]$. It is shown through simulation results that our proposed algorithm has effective control performance on the CVP system under DoS attacks and can effectively reduce the number of event triggers.

6. Conclusion

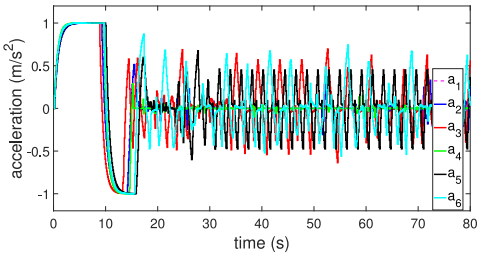
The DETM-based DMPC algorithm for heterogeneous CVP system under DoS attacks has been investigated in this paper. Firstly, a DETM was designed to reduce the frequency of data exchange between vehicles in the CVP system. Then, robust constraint was designed in the DMPC algorithm to deal with uncertainties in CVP systems. Whereafter, a packet replenishment mechanism was designed to ensure the integrity and effectiveness of information interaction. Sufficient conditions were given to guarantee the recursive feasibility of the DETM-based DMPC algorithm, and it was shown that the CVP system under this algorithm is ISPS under DoS attacks and external disturbance. Finally, the effectiveness of the algorithm was verified by numerical simulation based on MATLAB. However, the drawback of the control strategy in this paper is that it does not consider the impact of time-varying spacing policy and time-delays. In our future work, physical failure of motors in connected vehicles [51] should be considered together with the cyber attacks, which can provide the unified security of connected vehicles.



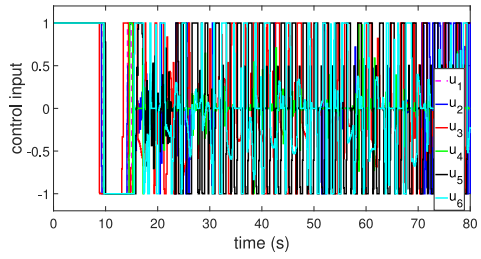
(a) Position trajectories.



(b) Velocity trajectories.



(c) Acceleration trajectories.



(d) Control input trajectories.

Fig. 6. The comparative simulation when $\Psi_{\max} = 67$.

CRediT authorship contribution statement

Hao Zeng: Writing – original draft, Investigation. **Zehua Ye:** Methodology. **Dan Zhang:** Writing – review & editing, Supervision, Funding acquisition, Conceptualization.

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.

Acknowledgments

This work was partially supported by the National Natural Science Foundation of China under Grant No. 62322315 and No. 61873237, the Zhejiang Provincial Natural Science Foundation of China under Grant No. LR22F030003.

References

[1] Ren R, Li H, Han T, Tian C, Zhang C, Zhang J, et al. Vehicle crash simulations for safety: Introduction of connected and automated vehicles on the roadways. Accid Anal Prev 2023;186:107021.
[2] Yang F, Gu Z, Hua L, Yan S. A resource-aware control approach to vehicle platoons under false data injection attacks. ISA Trans 2022;131:367–76.
[3] Mousavinejad E, Vlacic L. Secure platooning control of automated vehicles under cyber attacks. ISA Trans 2022;127:229–38.
[4] Liu Y, Yao D, Li H, Lu R. Distributed cooperative compound tracking control for a platoon of vehicles with adaptive NN. IEEE Trans Cybern 2022;52(7):7039–48.
[5] Chen M, Yan M. How to protect smart and autonomous vehicles from stealth viruses and worms. ISA Trans 2023;141:52–8.
[6] Parkinson S, Ward P, Wilson K, Miller J. Cyber threats facing autonomous and connected vehicles: Future challenges. IEEE Trans Intell Transp Syst 2017;18(11):2898–915.
[7] Wu C, Pan W, Staa R, Liu J, Sun G, Wu L. Deep reinforcement learning control approach to mitigating actuator attacks. Automatica 2023;152:110999.
[8] Cheng J, Wu Y, Wu Z-G, Yan H. Nonstationary filtering for fuzzy Markov switching affine systems with quantization effects and deception attacks. IEEE Trans Syst Man Cybern: Syst 2022;52(10):6545–54.
[9] Cheng J, Wang Y, Park JH, Cao J, Shi K. Static output feedback quantized control for fuzzy Markovian switching singularly perturbed systems with deception attacks. IEEE Trans Fuzzy Syst 2022;30(4):1036–47.
[10] Cheng J, Huang W, Park JH, Cao J. A hierarchical structure approach to finite-time filter design for fuzzy Markov switching systems with deception attacks. IEEE Trans Cybern 2022;52(8):7254–64.
[11] Xie M, Ding D, Ge X, Han Q-L, Dong H, Song Y. Distributed platooning control of automated vehicles subject to replay attacks based on proportional integral observers. IEEE/CAA J Autom Sin 2022;1–13.
[12] Xu X, Li X, Dong P, Liu Y, Zhang H. Robust reset speed synchronization control for an integrated motor-transmission powertrain system of a connected vehicle under a replay attack. IEEE Trans Veh Technol 2021;70(6):5524–36.
[13] Chen P, Zhang D, Yu L, Yan H. Dynamic event-triggered output feedback control for load frequency control in power systems with multiple cyber attacks. IEEE Trans Syst Man Cybern: Syst 2022;52(10):6246–58.
[14] Zhang D, Ye Z, Feng G, Li H. Intelligent event-based fuzzy dynamic positioning control of nonlinear unmanned marine vehicles under DoS attack. IEEE Trans Cybern 2022;52(12):13486–99.
[15] Mokari H, Firouzmand E, Sharifi I, Doustmohammadi A. Resilient control strategy and attack detection on platooning of smart vehicles under DoS attack. ISA Trans 2024;144:51–60.
[16] Ngo V-T, Liu Y-C. Distributed consensus control of networked robotic systems with dynamic leader under time-varying delays and Denial-of-Service attacks. IEEE Access 2022;10:92663–72.
[17] Ye Z, Zhang D, Feng G, Yan H. Finite-time consensus of leader-following MASs under DoS attacks. IEEE Control Syst Lett 2023;7:3409–14.
[18] Yang H, Ju S, Xia Y, Zhang J. Predictive cloud control for networked multiagent systems with quantized signals under DoS attacks. IEEE Trans Syst Man Cybern: Syst 2021;51(2):1345–53.
[19] Guo X-G, Liu P-M, Wu Z-G, Zhang D, Ahn CK. Hybrid event-triggered group consensus control for heterogeneous multiagent systems with tvnud faults and stochastic FDI attacks. IEEE Trans Autom Control 2023;68(12):8013–20.
[20] Abdollahi Biron Z, Dey S, Pisu P. Real-time detection and estimation of Denial of Service attack in connected vehicle systems. IEEE Trans Intell Transp Syst 2018;19(12):3893–902.
[21] Zhao N, Zhao X, Xu N, Zhang L. Resilient event-triggered control of connected automated vehicles under cyber attacks. IEEE/CAA J Autom Sin 2023;10(12):2300–2.
[22] Ge X, Han Q-L, Wu Q, Zhang X-M. Resilient and safe platooning control of connected automated vehicles against intermittent Denial-of-Service attacks. IEEE/CAA J Autom Sin 2023;10(5):1234–51.
[23] Li Z, Zhao H, Wang Y, Ren Y, Chen Z, Chen C. Adaptive event-triggered control for almost sure stability for vehicle platooning under interference and stochastic attacks. ISA Trans 2023;138:120–32.
[24] Zhang D, Shen Y-P, Zhou S-Q, Dong X-W, Yu L. Distributed secure platoon control of connected vehicles subject to DoS attack: Theory and application. IEEE Trans Syst Man Cybern: Syst 2021;51(11):7269–78.
[25] Merco R, Ferrante F, Pisu P. A hybrid controller for DoS-resilient string-stable vehicle platoons. IEEE Trans Intell Transp Syst 2021;22(3):1697–707.

[26] Tan G, Ren H, Zhang B, Deng F. Event-triggered control strategy based on absolute velocity and relative position measurements for second-order nonlinear multi-agent systems under DoS attacks. Neurocomputing 2024;574:127239.
[27] Lv G, Peng Z, Li Y, Liu L, Wang D. Barrier-certified model predictive cooperative path following control of connected autonomous surface vehicles. IEEE Trans Netw Sci Eng 2023;10(6):3354–67.
[28] Kennedy JM, Heinovski J, Quevedo DE, Dressler F. Centralized model predictive control with human-driver interaction for platooning. IEEE Trans Veh Technol 2023;72(10):12664–80.
[29] Feng S, Sun H, Zhang Y, Zheng J, Liu HX, Li L. Tube-based discrete controller design for vehicle platoons subject to disturbances and saturation constraints. IEEE Trans Control Syst Technol 2020;28(3):1066–73.
[30] Li Z, Xu H, Lin Z, Dong L, Chen Y. Event-triggered robust distributed output feedback model predictive control for nonlinear MASs against false data injection attacks. ISA Trans 2023;141:197–211.
[31] R. R, S.J. M, Jacob J. Dynamic consensus of linear multi-agent system using self-triggered distributed model predictive control. ISA Trans 2023;142:177–87.
[32] Chen J, Wei H, Zhang H, Shi Y. Asynchronous self-triggered stochastic distributed MPC for cooperative vehicle platooning over vehicular ad-hoc networks. IEEE Trans Veh Technol 2023;72(11):14061–73.
[33] Ju Z, Zhang H, Tan Y. Distributed stochastic model predictive control for heterogeneous vehicle platoons subject to modeling uncertainties. IEEE Intell Transp Syst Mag 2022;14(2):25–40.
[34] Ding B, Ge L, Pan H, Wang P. Distributed mpc for tracking and formation of homogeneous multi-agent system with time-varying communication topology. Asian J Control 2016;18(3):1030–41.
[35] Chen L, Zhan J, Zhang L. Distributed model predictive control of vehicle platoons under switching communication topologies. IMA J Math Control Inform 2023;dnad023.
[36] Zhu P, Jin S, Bu X, Hou Z. Distributed data-driven event-triggered fault-tolerant control for a connected heterogeneous vehicle platoon with sensor faults. IEEE Trans Intell Transp Syst 2023;1–12.
[37] Liu J, Wu L, Wu C, Luo W, Franquelo LG. Event-triggering dissipative control of switched stochastic systems via sliding mode. Automatica 2019;103:261–73.
[38] Yu T, Zhao Y, Wang J, Liu J. Event-triggered sliding mode control for switched genetic regulatory networks with persistent dwell time. Nonlinear Anal Hybrid Syst 2022;44:101135.
[39] Ye Z, Zhang D, Wu Z-G, Yan H. A3C-based intelligent event-triggering control of networked nonlinear unmanned marine vehicles subject to hybrid attacks. IEEE Trans Intell Transp Syst 2022;23(8):12921–34.
[40] Wen S, Guo G, Chen B, Gao X. Event-triggered cooperative control of vehicle platoons in vehicular ad hoc networks. Inform Sci 2018;459:341–53.
[41] Ge X, Xiao S, Han Q-L, Zhang X-M, Ding D. Dynamic event-triggered scheduling and platooning control co-design for automated vehicles over vehicular ad-hoc networks. IEEE/CAA J Autom Sin 2022;9(1):31–46.
[42] Chen J, Zhang H, Yin G. Distributed dynamic event-triggered secure model predictive control of vehicle platoon against DoS attacks. IEEE Trans Veh Technol 2023;72(3):2863–77.
[43] Zheng Y, Li SE, Li K, Ren W. Platooning of connected vehicles with undirected topologies: Robustness analysis and distributed h-infinity controller synthesis. IEEE Trans Intell Transp Syst 2018;19(5):1353–64.
[44] Wu C, Wu L, Liu J, Jiang Z-P. Active defense-based resilient sliding mode control under Denial-of-Service attacks. IEEE Trans Inf Forensics Secur 2020;15:237–49.
[45] Ye Z, Zhang D, Wu Z-G. Adaptive event-based tracking control of unmanned marine vehicle systems with DoS attack. J Franklin Inst 2021;358(3):1915–39.
[46] De Persis C, Tesi P. Input-to-state stabilizing control under Denial-Of-Service. IEEE Trans Autom Control 2015;60(11):2930–44.
[47] Ye Z, Zhang D, Deng C, Yan H, Feng G. Finite-time resilient sliding mode control of nonlinear UMV systems subject to DoS attacks. Automatica 2023;156:111170.
[48] Ni H, Xu Z, Cheng J, Zhang D. Robust stochastic sampled-data-based output consensus of heterogeneous multi-agent systems subject to random DoS attack: A Markovian jumping system approach. Int J Control Autom Syst 2019;17:1687–98.
[49] Dai Y, Li M, Zhang K, Shi Y. Robust and resilient distributed mpc for cyber-physical systems against DoS attacks. IEEE Trans Ind Cyber-Phys Syst 2023;1:44–55.
[50] Sun Q, Chen J, Shi Y. Event-triggered robust mpc of nonlinear cyber-physical systems against DoS attacks. Sci China Inf Sci 2022;65(1):110202.
[51] Chen Y, Zhang D, Yan R. Domain adaptation networks with parameter-free adaptively rectified linear units for fault diagnosis under variable operating conditions. IEEE Trans Neural Netw Learn Syst 2023;1–14.

ISA Transactions 153 (2024) 1–12

Contents lists available at ScienceDirect

ISA Transactions

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

Research article

Dynamic event-triggering-based distributed model predictive control of heterogeneous connected vehicle platoon under DoS attacks

Hao Zeng, Zehua Ye, Dan Zhang *

Research Center of Automation and Artificial Intelligence, Zhejiang University of Technology, Hangzhou, 310023, PR China

ARTICLE INFO

Keywords:
Heterogeneous CVP
DMPC
DoS attacks
DETM
ISPS

ABSTRACT

This paper is concerned with the distributed model predictive control (DMPC) for heterogeneous connected vehicle platoon (CVP) under denial-of-service (DoS) attacks. Firstly, a dynamic event-triggering mechanism (DETM) based on the information interaction between vehicles is proposed to reduce the communication and computational burdens. Due to the fact that the triggering moment for each vehicle cannot be synchronized and DoS attacks can break the communication between vehicles, a packet replenishment mechanism is designed to ensure the integrity and effectiveness of information interaction. Then, the effect of external disturbance is handled by adding robustness constraints to the DMPC algorithm. In addition, the recursive feasibility of the DMPC algorithm and input-to-state practical stability (ISPS) of the CVP control system are demonstrated. Finally, the effectiveness of the algorithm is verified by simulation and comparison results.

1. Introduction

With the development of the economy and technology, the number of vehicles has increased rapidly, raising the probability of traffic congestion and traffic accidents [1]. The control issue of the connected vehicle platoon (CVP) system aims to keep vehicles traveling at a desired longitudinal speed and spacing, which is regarded to be an effective technical solution to solve the above problems [2]. Studies have shown that CVP control can reduce the air resistance of following vehicles during traveling, effectively reduce fuel consumption, and improve the safety of traffic [3,4]. Therefore, the control problem of CVP system has attracted extensive attention in intelligent transport systems. The CVP system uses the IEEE 802.11p protocol for short-range communication and C-V2X/5G technology for long-range communication [5]. In this scenario, the CVP system is a complex cyber–physical system with deep integration of computation, communication, control, and vehicle.

As the CVP system transmits information over networks, cyber-attacks on such vehicles are becoming increasingly prevalent as the growing openness of networks [6,7]. Thus, the security of the CVP system is worth investigating deeply. There are three representative types of cyber-attacks, which can be broadly categorized as deception attacks [8–10], replay attacks [11,12], and denial-of-service (DoS) attacks [13–15]. DoS attacks are the most prevalent and destructive form of cyber-attacks [16,17]. When DoS attacks occur, the adversary occupies the system's communication and storage units by sending numerous illegal request services, which causes the system to be unable to process regular request services sent by legitimate users [18,19]. In this case, DoS attacks can break communication channels in the CVP system, which can degrade the control performance of the CVP system and even lead to collision.

The security control problem of CVP system under DoS attacks has been extensively studied in the past few years. For instance, a sliding mode observer was designed to detect whether DoS attacks occur in [20], and the impact of DoS attacks on CVP system was illustrated through simulation. In [21], a robust event-triggering mechanism (ETM) for the CVP system was designed to mitigate the impact of DoS attacks and reduce the network burden. In [22], a distributed resilient control law was devised for the heterogeneous CVP system under DoS attacks, and the effectiveness of the algorithm was verified through numerical simulations. In [23], a resilient adaptive event-triggering platoon control strategy was proposed for the CVP system under DoS attacks to enable vehicles to maintain the prescribed spacing. In our earlier work [24], the controller design for the CVP system under DoS attacks was analyzed using a switched system method and the effect of DoS attacks parameters on the system's performance. In [25], the security control problem of CVP system under DoS attacks was investigated and the controller gains were calculated based on linear matrix inequalities. In [26], a control protocol based on ETM that can achieve leader-following consensus was proposed, and the effectiveness of the proposed distributed security control protocol was verified by the numerical simulation of CVP system. Although the above results are very effective for CVP system subject to DoS attacks, the constraint

* Corresponding author.
E-mail address: [redacted] Zhang).

https://doi.org/10.1016/j.isatra.2024.07.011
Received 24 February 2024; Received in revised form 11 June 2024; Accepted 5 July 2024
Available online 15 July 2024

problem has yet to be well studied in the above studies. Instead, the parameters of vehicles in the CVP system are usually constrained during traveling, see, e.g., speed and control input. Thus, it is necessary to investigate the resilient control problem of the CVP system in the constrained situation.

Model predictive control (MPC) algorithm represents a viable solution to the issue of control systems that are constrained by inputs and states [27]. The MPC algorithm has been widely applied in various fields, and those comprehensive results on MPC can roughly classify into three types: centralized MPC [28], decentralized MPC [29], and distributed MPC (DMPC) [30–32]. The centralized MPC shows proficient optimization capabilities, but it is only suitable for small-scale systems with low computational requirements. The decentralized MPC reduces the computational burden by eliminating the need for connections between subsystems. However, the performance of the system may be degraded. The DMPC realizes the optimal control of the system by decomposing the large-scale online optimization problem and the information interaction between subsystems, which is proved to be suitable for solving control problems of the large-scale system. Therefore, the DMPC received attractive research attention in the field of the CVP system due to its outstanding performance and capability to deal with constraints efficiently. In [33], a distributed stochastic MPC algorithm was proposed for the vehicle dynamic system with modeling uncertainty, and it was proven that the tracking errors in the CVP system asymptotically converge to zero under that algorithm. In [34], a DMPC algorithm was introduced to address the challenges in multi-agent systems with time-varying communication topology, and the effects of changing communication topology on stability were mitigated efficiently. In [35], two different DMPC algorithms were proposed to ensure the asymptotic stability and string stability of the CVP system under a switched communication topology.

Although the above methods can be adopted to solve the constraint problem in the CVP system, the communication constraint problem has not been well solved. In reality, the communication resource is usually limited for a large-scale vehicle network [36]. The ETM can effectively decrease the volume of processed data while conserving network resources, which has been extensively studied in literature [37–39]. There are two types of ETM: static ETM (SETM) and dynamic ETM (DETM). Compared with the SETM, the DETM can further reduce the number of triggers by introducing dynamic variables. Thus, DETM has a broader application in the CVP system. Recently, a DETM was proposed in [40] to dynamically adjust the threshold parameter by the measurement error, and thereby significantly reducing the communication burden of the CVP system. In [41], a DETM with threshold parameter varying according to vehicle state and bandwidth state was proposed, and simulation results demonstrated the significant reduction in bandwidth consumption achieved by the method. Although the above results effectively reduce the number of triggers, they do not consider the situation where DoS attacks can disrupt communication. Therefore, it is urgent to design a resilient security control algorithm and DETM in order to reduce the communication burden of CVP system under DoS attacks.

On the basis of the above discussion, this paper is concerned with the DETM-based DMPC problem for CVP system under DoS attacks. A heterogeneous CVP system with external disturbance is first established, and a DETM with dynamically adjusted threshold parameters is proposed to save communication resources. Then, sufficient conditions to ensure the feasibility of the DMPC algorithm are given, and the stability of the CVP system under DoS attack is analyzed under the DMPC algorithm. In the section of simulation, a CVP system with six vehicles is finally taken as an example to verify the effectiveness of the designed method. The main contributions of this paper can be summarized as follows:

(1) A new DETM is designed. The threshold parameters of the DETM can be dynamically adjusted by the error between the actual state of the ith vehicle and the predicted state in the buffer. The threshold parameter will decrease as the error between the actual state of the ith vehicle and the predicted state in the buffer becomes larger. In the simulation, the proposed DETM reduces the number of triggers by 46.6% in the time interval $[0, 800]$ compared with the existing DETM. Therefore, the proposed DETM can significantly reduce the number of triggers and network burden.

(2) A DMPC algorithm is proposed. The virtual leading vehicle generates reference state trajectory for the CVP system to obtain the tracking error equation for each vehicle. The effect of external disturbances on the CVP system is handled by adding robust constraints to the tracking error of each vehicle in the DMPC algorithm. The recursive feasibility of DMPC and the input-to-state practical stability (ISPS) of the CVP system are analyzed based on the newly proposed DETM.

(3) A packet replenishment mechanism is designed. The packet replenishment mechanism can ensure the integrity and effectiveness of information interaction under DETM in the presence of DoS attacks. When DoS attacks occur, input packets stored in the buffer are used to control the vehicle. Compared with the zero input mechanism, the hold input mechanism in this paper compensates for the impact of DoS attacks on the CVP system.

Notations: In this paper, R is the set of all real numbers and $R^{m\times n}$ denotes the $m \times n$ dimensional matrix. N^+ denotes the set of non-zero natural numbers, I_m denotes the m-dimensional identity matrix. Define $\|x\|^2 = x^T x$ and $\|x\|_P^2 = x^T Px$, where $x \in R^{m\times 1}$ and $P \in R^{m\times m}$. Define $\lambda_{\max}(P)$ and $\lambda_{\min}(P)$ denote the maximum and minimum eigenvalues of the matrix P.

2. Preliminaries and problem formulation

This section elaborates on some basis and problem description. The system structure is shown in Fig. 1. The data is transmitted according to the communication topology when the event-triggering condition is satisfied. The communication channels will be jammed when DoS attacks occur.

2.1. Communication graph

The CVP system can have many different communication topologies to adapt to the requirements of various application scenarios. The communication interactions among vehicles can be described by graph theory, which can be represented as a directed graph ζ. For ζ, the adjacency matrix $\mathcal{A}_{\mathcal{N}}$ is defined as $\mathcal{A}_{\mathcal{N}} = [a_{ij}] \in R^{\mathcal{N}\times\mathcal{N}} (i, j = 1, 2, \dots, \mathcal{N})$, where $a_{ij} = 1$ represents that the ith vehicle can receive data from the jth vehicle, otherwise $a_{ij} = 0$. Define $\mathbb{C}_i$ as the set of vehicles, where $\mathbb{C}_i = \{j | a_{ij} = 1\}$.

2.2. Vehicle models

A CVP system with $\mathcal{N}$ vehicles is considered in this work. The leading vehicle is indexed as 1, and the following vehicles are indexed from 2 to $\mathcal{N}$. It is assumed that the virtual leading vehicle operates at a fixed speed to generate reference position and speed for the vehicles in the platoon. The discrete-time longitudinal dynamics model of the virtual leading vehicle can be represented as

$$\begin{cases} p_r(k+1) = p_r(k) + v_r(k)\Delta T \\ v_r(k+1) = v_r(k) \\ a_r(k+1) = 0 \end{cases} \tag{1}$$

where $p_r(k)$, $v_r(k)$, and $a_r(k)$ represent the position, velocity, and acceleration of the virtual leading vehicle, respectively. ΔT denotes the sampling period.

The linearized discrete-time longitudinal dynamic equation for the vehicle is given by [42]

$$x_i(k+1) = A_i x_i(k) + B_i u_i(k) + C_i \omega_i(k) \tag{2}$$

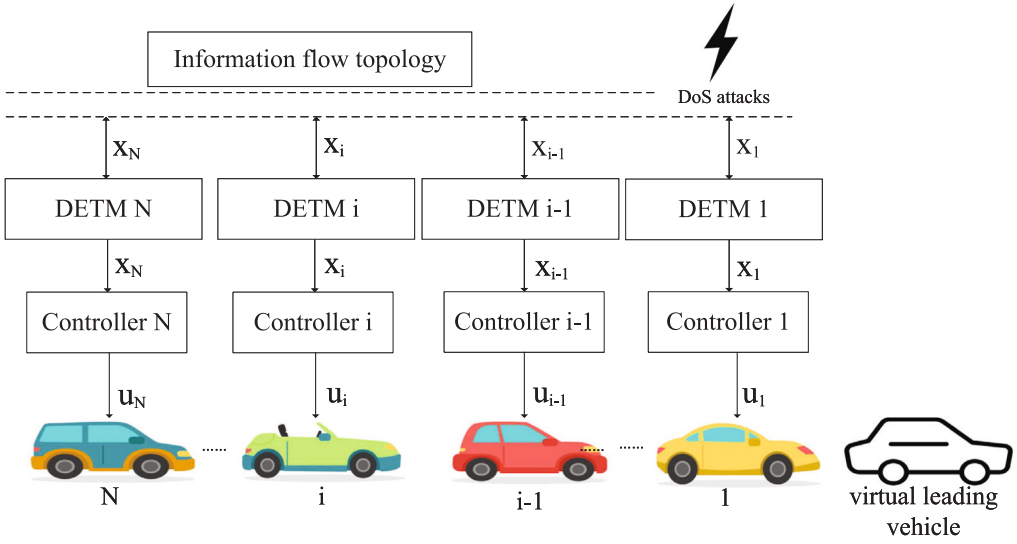


Fig. 1. System structure.

where $x_i(k) = \begin{bmatrix} p_i(k) & v_i(k) & a_i(k) \end{bmatrix}^T \in R^{3\times 1}$, $u_i(k) \in R$, and $\omega_i(k) \in R$ are the state, control input, and external disturbance of ith vehicle, respectively, $i = 1, 2, \ldots, \mathcal{N}$. In this paper, the external disturbance is assumed to be bounded, i.e., $\|\omega_i(k)\|^2 \leqslant \|W\|^2$. $p_i(k)$, $v_i(k)$ and $a_i(k)$ represent the position, velocity and acceleration of the ith vehicle, respectively. $A_i = \begin{bmatrix} 1 & \Delta T & 0 \\ 0 & 1 & \Delta T \\ 0 & 0 & 1-\frac{\Delta T}{\tau_i} \end{bmatrix}$, $B_i = \begin{bmatrix} 0 \\ 0 \\ \frac{\Delta T}{\tau_i} \end{bmatrix}$ and $C_i = \begin{bmatrix} 0 \\ 0 \\ \Delta T \end{bmatrix}$ are constant matrices. τ_i denotes the engine inertia time constant of the ith vehicle.

Remark 1. The studies of CVP system based on this linearized vehicle model have received much attention, see, e.g., [41–43]. In this paper, we will use this linearized vehicle model as the control plant, and the main goal is to design the cooperative control strategy for CVP system subject to DoS attacks and constraints.

2.3. DoS attacks

In this paper, it is assumed that DoS attacks can occur randomly on any communication channel of the CVP system, and the adversary will block the data transmission among the vehicles. Define $\{\mathcal{L}_i\}_{i\in \mathrm{N}^+}$ as the instant when the ith DoS attacks occur and n_i denote the duration of the ith DoS attacks, where $n_i > 0$. Thus, the activity time of DoS attacks in the interval $[0, k]$ can be represented as

$$\Gamma(0,k) = \bigcup_{i\in \mathrm{N}^+} [\mathcal{L}_i + n_i) \bigcap [0,k] \tag{3}$$

Define $\Gamma_{tot}(0,k)$ as the length of $\Gamma(0,k)$, and then the following assumptions are introduced to describe the DoS attacks.

Assumption 1 ([44]). For DoS attacks duration, there exist constants σ and T_a such that

$$\Gamma_{tot}(0,k) \leqslant \sigma + \frac{k}{T_a} \tag{4}$$

holds for all $k \in N^+$, where $\sigma \geqslant 0$ and $T_a \geqslant 1$.

Assumption 2 ([42]). It is assumed that $\Psi_{\max} = \sigma + \frac{k}{T_a}$ is the maximum total duration of DoS attacks in the time interval $[0, k]$, the maximum duration of a single DoS attacks is N_a.

Remark 2. The modeling of DoS attacks has been investigated in many articles [44–48]. The above two assumptions have practical significance because adversaries may need to hide their attack strategy to avoid detection, i.e., they may not launch an attack at every time instant, and the attack is also subject to power consumption, which is always limited.

2.4. Problem description

The objective of this paper is to design a resilient controller such that all vehicles can track the state of the virtual leading vehicle and the desired spacing between two contiguous vehicles in the CVP system is guaranteed, which can be represented as

$$\begin{cases} \lim_{k\to\infty} \left(p_{i-1}(k) - p_i(k) - d\right) = 0 \\ \lim_{k\to\infty} \left(v_i(k) - v_r(k)\right) = 0 \\ \lim_{k\to\infty} \left(a_i(k) - a_r(k)\right) = 0 \end{cases} \tag{5}$$

The parameters of vehicles in the CVP system are usually constrained during traveling. For instance, the constraints for speed and acceleration are usually required for driving safety and passenger comfort, and the input constraint is limited by the physical conditions of the vehicle, which can be represented as

$$\begin{cases} v_{i,\min} \leqslant v_i(k) \leqslant v_{i,\max} \\ a_{i,\min} \leqslant a_i(k) \leqslant a_{i,\max} \\ u_{i,\min} \leqslant u_i(k) \leqslant u_{i,\max} \end{cases} \tag{6}$$

where $v_{i,\min}$, $a_{i,\min}$, and $u_{i,\min}$ denote the minimum values of the velocity, acceleration, and control input, respectively. $v_{i,\max}$, $a_{i,\max}$, and $u_{i,\max}$ denote the maximum values of the velocity, acceleration, and control input, respectively. The constraints on the system state and control input can be expressed as $x_i(k) \in \mathrm{X}_i \subseteq R^{3\times 1}$ and $u_i(k) \in \mathcal{U}_i \subseteq R$.

Define the tracking error of the ith vehicle as

$$e_i(k) = \begin{bmatrix} p_i(k) - p_r(k) - d_{ir} \\ v_i(k) - v_r(k) \\ a_i(k) - a_r(k) \end{bmatrix} \tag{7}$$

where $d_{ir} = i \times d$ denotes the desired spacing between ith vehicle and the virtual leading vehicle. Thus, the tracking error equation can be written as

$$e_i(k+1) = A_i e_i(k) + B_i u_i(k) + C_i \omega_i(k) \tag{8}$$

Similar to those state and control constraints, the error constraints in the tracking error Eq. (8) can be represented as $e_i(k) \in \chi_i \subseteq R^{3\times 1}$.

The following assumption is important for the control algorithm design and stability analysis.

Assumption 3 ([49]). For the system $e_i(k+1) = A_i e_i(k) + B_i u_i(k)$, the terminal set $\mathcal{H}(\eta_i)$ is defined as $\mathcal{H}(\eta_i) = \left\{ e_i \middle| \|e_i(k)\|_{P_i}^2 \leqslant {\eta_i}^2 \right\}$. When $e_i(k) \in \mathcal{H}(\eta_i)$, for given constant $\eta_i > 0$, state weighting matrix Q_i, and control weighting matrix R_i, there exist a positive definite matrix P_i and a feedback control law K_i such that

$$\|e_i(k+1)\|_{P_i}^2 - \|e_i(k)\|_{P_i}^2 \leqslant -\|e_i(k)\|_{Q_i + K_i^T R_i K_i}^2 \tag{9}$$

holds.

Remark 3. When $e_i(k) \in \mathcal{H}(\eta_i)$, P_i can be calculated from the Riccati equation ${A_i}^T P_i A_i - P_i - {A_i}^T P_i B_i ({B_i}^T P_i B_i + R_i)^{-1} {B_i}^T P_i A_i + Q_i = 0$ and K_i can be calculated by $K_i = ({B_i}^T P_i B_i + R_i)^{-1} {B_i}^T P_i A_i$.

3. Dynamic event-triggering and distributed model predictive control

3.1. Dynamic event-triggering mechanism

Frequent inter-vehicle communication increases the communication and computation burden. Therefore, a novel DETM is designed to reduce inter-vehicle communication.

Assuming that k_i^d is the dth triggering moment of ith vehicle, the next triggering time instant of DETM is determined as

$$k_i^{d+1} = \inf\left\{ t \in N^+ | \Phi > 0 \right\} \tag{10}$$

where $\Phi = \left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm1}}^2 - \gamma_i(k_i^d + t)\phi_i$, $\Pi_{1i}\left(k_i^d + t\right) = x_i\left(k_i^d + t\right) - x_i^B\left(k_i^d + t | k_i^d\right)$, $\gamma_i(k_i^d + t) = \Pi_{2i}(k_i^d + t)\delta_{1i}(k_i^d + t) + \left(1 - \Pi_{2i}(k_i^d + t)\right)\delta_{2i}(k_i^d + t)$, $\Pi_{2i}\left(k_i^d + t\right) = tansig\left[\Pi_{3i}\left(k_i^d + t\right)\right]$, $\Pi_{3i}\left(k_i^d + t\right) = \sum_{j \in \mathbb{C}_i} \left[x_i(k_i^d + t) - {x_j}^B(k_i^d + t | k_i^d) - d_{i,j}\right]$, ϕ_i is a positive scalar, Q_{etm1} is a positive matrix. $\Pi_{1i}\left(k_i^d + t\right)$ denotes the error between the actual state and the predicted state of the ith vehicle at k_i^d. $\Pi_{3i}\left(k_i^d + t\right)$ denotes the error between the actual state of the ith vehicle and the predicted state of its neighbors at k_i^d, $d_{i,j} = \begin{bmatrix} d_{ij} & 0 & 0 \end{bmatrix}^T$. $x_i^B\left(k_i^d + t | k_i^d\right)$ and $x_j^B\left(k_i^d + t | k_i^d\right)$ are the predicted state of ith vehicle and the predicted state of the neighboring vehicles in the received data packet at the moment k_i^d, the specific form of the data packet will be elaborated in Section 3.3. $\delta_{1i}(k_i^d + t)$ and $\delta_{2i}(k_i^d + t)$ are two online update threshold parameters, which are defined as

$$\delta_{1i}(k_i^d + t + 1) = \frac{\delta_{1i}(k_i^d + t)}{1 + \varepsilon_{1i}\delta_{1i}(k_i^d + t)\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2} \tag{11a}$$

$$\delta_{2i}(k_i^d + t + 1) = \frac{\delta_{iM} + \varepsilon_{2i}\delta_{2i}(k_i^d + t)\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2}{1 + \varepsilon_{2i}\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2} \tag{11b}$$

where $\varepsilon_{1i} \geqslant 0$, $\varepsilon_{2i} \geqslant 0$ and $0 \leqslant \delta_{im} \leqslant \delta_{iM} \leqslant 1$ are some threshold parameters for offline design, Q_{etm2} is a positive matrix. The following theorem introduce the key properties of our proposed DETM condition.

Theorem 1. *Given positive scalars $\varepsilon_{1i} > 0$, $\varepsilon_{2i} > 0$, $\delta_{iM} \geqslant \delta_{im} \geqslant 0$, $0 \leqslant \delta_{1i}(0) \leqslant \delta_{im}$, $\delta_{im} \leqslant \delta_{2i}(0) \leqslant \delta_{iM}$ and positive definite matrix Q_{etm2}, the sequence $\left\{\delta_{1i}(k_i^d)\right\}$ is monotonically non-increasing and satisfies $0 \leqslant \delta_{1i}(k_i^d) \leqslant \delta_{1i}(0) \leqslant \delta_{1m}$, the sequence $\left\{\delta_{2i}(k_i^d)\right\}$ is monotonically non-decreasing and satisfies $\delta_{im} \leqslant \delta_{2i}(0) \leqslant \delta_{2i}(k_i^d) \leqslant \delta_{iM}$ and the dynamic threshold parameter $\gamma_i(k_i^d)$ satisfies $0 \leqslant \delta_{1i}(k_i^d) \leqslant \gamma_i(k_i^d) \leqslant \delta_{2i}(k_i^d) \leqslant \delta_{iM}$.*

Proof. First, we analyze the monotonicity of $\left\{\delta_{1i}(k_i^d)\right\}$ as

$$\begin{aligned}
&\delta_{1i}(k_i^d + t + 1) - \delta_{1i}(k_i^d + t) \\
&= \frac{\delta_{1i}(k_i^d + t)}{1 + \varepsilon_{1i}\delta_{1i}(k_i^d + t)\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2} - \delta_{1i}(k_i^d + t) \\
&= \frac{-{\delta_{1i}}^2(k_i^d + t)\varepsilon_{1i}\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2}{1 + \varepsilon_{1i}\delta_{1i}(k_i^d + t)\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2} \leqslant 0
\end{aligned} \tag{12}$$

It can be obtained that the sequence $\left\{\delta_{1i}(k_i^d)\right\}$ is monotonically non-decreasing and $\delta_{1i}(k_i^d) \geqslant 0$.

Then it follows from $\left\{\delta_{2i}(k_i^d)\right\}$ that

$$\begin{aligned}
&\delta_{2i}(k_i^d + t + 1) - \delta_{iM} \\
&= \frac{\delta_{iM} + \varepsilon_{2i}\delta_{2i}(k_i^d + t)\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2}{1 + \varepsilon_{2i}\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2} - \delta_{iM} \\
&= \frac{\varepsilon_{2i}\left[\delta_{2i}(k_i^d + t) - \delta_{iM}(k_i^d + t)\right]\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2}{1 + \varepsilon_{2i}\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2} \\
&\leqslant 0
\end{aligned} \tag{13}$$

which implies $\delta_{2i}(k_i^d) \leqslant \delta_{iM}$. Applying the similar derivation of (12) to the $\left\{\delta_{2i}(k_i^d)\right\}$, one can obtain that

$$\begin{aligned}
&\delta_{2i}(k_i^d + t + 1) - \delta_{2i}(k_i^d + t) \\
&= \frac{\delta_{iM} + \varepsilon_{2i}\delta_{2i}(k_i^d + t)\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2}{1 + \varepsilon_{2i}\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2} - \delta_{2i}(k_i^d + t) \\
&= \frac{\delta_{iM} - \delta_{2i}(k_i^d + t)}{1 + \varepsilon_{2i}\left\| \Pi_{1i}\left(k_i^d + t\right) \right\|_{Q_{etm2}}^2} \geqslant 0
\end{aligned} \tag{14}$$

It means that the sequence $\left\{\delta_{2i}(k_i^d)\right\}$ is monotonically non-decreasing.

As for $\gamma_i(k_i^d)$, the following inequalities hold

$$\begin{aligned}
&\gamma_i(k_i^d + t) - \delta_{1i}(k_i^d + t) \\
&\quad = \left[1 - \Pi_{2i}\left(k_i^d + t\right)\right]\left(\delta_{2i}(k_i^d + t) - \delta_{1i}(k_i^d + t)\right) \geqslant 0
\end{aligned} \tag{15}$$

$$\begin{aligned}
&\gamma_i(k_i^d + t) - \delta_{2i}(k_i^d + t) \\
&\quad = \Pi_{2i}\left(k_i^d + t\right)\left[\delta_{1i}(k_i^d + t) - \delta_{2i}(k_i^d + t)\right] \leqslant 0
\end{aligned} \tag{16}$$

It follows from (15) and (16) that $\gamma_i(k_i^d)$ satisfies $0 \leqslant \delta_{1i}(k_i^d) \leqslant \gamma_i(k_i^d) \leqslant \delta_{2i}(k_i^d) \leqslant \delta_{iM}$. This completes the proof.

Remark 4. The threshold parameters of the DETM can be dynamically adjusted by the error between the actual state of the ith vehicle and the predicted state in the buffer. The threshold parameter will decrease as the error between the actual state of the ith vehicle and the predicted state in the buffer becomes larger. It can effectively reduce the communication and computation burden. When DoS attacks occur, the error between the actual state and the predicted state of the ith vehicle will increase due to external disturbance and the inability to solve the optimization problem, and the error between the predicted state of the ith vehicle and the neighbor vehicle will also increase. In this case, the value of $\Pi_{2i}\left(k_i{}^d + t\right)$ will become larger, the value of $\delta_{1i}(k_i^d + t)$ will become smaller, and the value of $\gamma_i(k_i^d + t)$ will therefore become smaller. The ith vehicle will trigger more frequently as the threshold parameter of the DTEM becomes smaller, thus enabling the ith vehicle to achieve cooperative control with the neighbor vehicle.

3.2. Distributed model predictive control

In this section, we are on the stage to discuss the DMPC design. For each vehicle in the CVP system, we assume that the prediction horizon of the finite horizon optimization problem is N. First, the following three types of sequences are defined as

1. $\tilde{x}_i(k_i^d + t | k_i^d)$ and $\tilde{u}_i(k_i^d + t | k_i^d)$ are the predicted state sequence and the predicted control input sequence.
2. ${x_i}^*(k_i^d + t | k_i^d)$ and ${u_i}^*(k_i^d + t | k_i^d)$ are the optimal state sequence and input sequence generated under the finite horizon optimization problem at moment k_i^d. The finite horizon optimization problem are defined later in this section.

3. ${x_i}^B(k_i^d+t|k_i^d)$ and ${u_i}^B(k_i^d+t|k_i^d)$ are the optimal state sequence and optimal input sequence stored in the buffer obtained by solving the finite time domain optimization problem at moment k_i^d.

The cost function of ith vehicle is defined as

$$J_i\left(\tilde{x}_i(k_i^d),\tilde{u}_i(k_i^d),X_i^a(k_i^d)\right)=J_{i1}\left(k_i^d\right)+J_{i2}\left(k_i^d\right)+V_{iN}\left(k_i^d\right) \tag{17}$$

where $J_{i1}(k_i^d)=\sum_{n=0}^{N-1}\left[\left\|\tilde{e}_i(k_i^d+n|k_i^d)\right\|_{Q_i}^2+\left\|\tilde{u}_i(k_i^d+n|k_i^d)\right\|_{R_i}^2\right]$, $J_{i2}(k_i^d)=\sum_{n=0}^{N-1}\sum_{j\in\mathbb{C}_i}\left\|\tilde{x}_i(k_i^d+n|k_i^d)-x_j^B(k_i^d+n|k_i^d)-d_{i,j}\right\|_{Q_{ij}}^2$, $V_{iN}(k_i^d)=\left\|\tilde{e}_i(k_i^d+N|k_i^d)\right\|_{P_i}^2$, $\tilde{e}_i(k_i^d+n|k_i^d)=\tilde{x}_i(k_i^d+n|k_i^d)-x_r(k_i^d+n)-d_{i,r}$, $J_{i1}(k_i^d)$ is the cost function of the tracking error and control input, $J_{i2}(k_i^d)$ is the cost function for the state error of the ith vehicle and its neighbors, $V_{iN}(k_i^d)$ is the terminal cost function, Q_{ij} is weighting matrix, $X_i^a(k_i^d)$ denotes the total number of data packets that ith vehicle can receive at k_i^d.

We design robustness constraints to the optimization problem for each vehicle, and the finite horizon optimization problem for ith vehicle can be expressed as

$$\min J_i(\tilde{x}_i(k_i^d),\tilde{u}_i(k_i^d),X_i^a(k_i^d))$$

s.t.

$$\|\tilde{e}_i(k_i^d+n|k_i^d)\|^2\in\left(1-\frac{n}{N}\varsigma_i\right)\|\chi_i\|^2 \tag{18a}$$

$$\tilde{u}_i(k_i^d+n|k_i^d)\in\mathcal{U}_i \tag{18b}$$

$$\tilde{x}_i(k_i^d+n+1|k_i^d)=A_i\tilde{x}_i(k_i^d+n|k_i^d)+B_i\tilde{u}_i(k_i^d+n|k_i^d) \tag{18c}$$

$$\|\tilde{e}_i(k_i^d+N|k_i^d)\|_{P_i}^2\le\alpha_i^2\varepsilon_i^2 \tag{18d}$$

for $n\in[0,N-1]$

where (18a) and (18d) are tightening state constraints and tightening terminal constraints, aiming to make the tracking error of the ith vehicle tighter. $\varsigma_i\in(0,1)$ and $\alpha_i\in(0,1)$ are robust constraint parameters. (18b) is the input constraint of the ith vehicle. The finite horizon optimization problem is established to minimize the cost function and the input to the system subject to the input constraints.

Remark 5. It is noted that the leading vehicle only needs to follow the state of the virtual leading vehicle. Thus, we assume that the leading vehicle can always carry out the finite horizon optimization problem to improve the operation efficiency in the CVP system.

Remark 6. The robustness constraint ensures that the system tracking error sequence has an upper bound on the decreasing function even in the external disturbance. The coordination of the entire CVP system is achieved by minimizing the cost function through a finite horizon optimization problem for each vehicle.

3.3. Buffer and data packet design

Due to the existence of DoS attacks and DETM, it is necessary to design the format of buffer and data packet. Since the condition of the event-triggering is related to the state information transmitted by its vehicle and the neighboring vehicles at the moment of triggering, this information should be stored in the form of data packets in the buffer. Considering the existence of DoS attacks, we use a lengthened sequence of state and control inputs in the data packet. The input sequence in the data packet is

$${U_i}^B(k_i^d+n|k_i^d)=\begin{cases}{u_i}^*(k_i^d+n|k_i^d), & n\in[0,N-1]\\ K_ie_i(k_i^d+n|k_i^d), & n\in\left[N,N+N_a-1\right]\end{cases} \tag{19}$$

For $n\in\left[0,N+N_a-1\right]$, the sequence of state in the data packet is

$${X_i}^B(k_i^d+n+1|k_i^d)=A{x_i}^*(k_i^d+n|k_i^d)+B{U_i}^B(k_i^d+n|k_i^d) \tag{20}$$

Since the event-triggering instant of each vehicle cannot be synchronized, thus the transmitted data is not necessarily the optimal state sequence and the optimal input sequence of the neighboring vehicles at the triggering moment. To ensure that the amount of data in the packet transmitted to the neighboring vehicles is more than or equal to N, we design the format of the data packet. Before the next triggering instant, the first data in the data packet is deleted in every sampling period, and the state and input data obtained through state feedback are added at the end. The real-time updating of data packets is an excellent way to ensure the integrity and validity of the transmitted data.

4. Main results

In this section, the recursive feasibility of the DETM-based DMPC algorithm proposed in this paper and the stability of the CVP system under DoS attacks are analyzed. The following definition is significant for the analysis of stability:

Definition 1 (*[50]*)**.** Considering the system (8), the external disturbance satisfies $\|\omega_i(k)\|^2\le\|W\|^2$, if there exists a function $V\left(e_i(k)\right)$, $\mathcal{K}_\infty$ class functions α_1, α_2, and ρ_1, a $\mathcal{K}$ class function ρ_2, constants $\beta_1\ge0$ and $\beta_2\ge0$ such that

$$\alpha_1(\|e_i(k)\|)\leqslant V(e_i(k))\leqslant\alpha_2(\|e_i(k)\|)+\beta_1 \tag{21}$$

$$V(e_i(k+1))-V(e_i(k))\leqslant-\rho_1(\|e_i(k)\|)+\rho_2(\|W\|)+\beta_2 \tag{22}$$

hold. Then the system (8) is input-to-state practical stability (ISPS).

4.1. Recursive feasibility analysis

It is assumed that the DETM-based DMPC algorithm proposed in the previous section is initially feasible. Recursive feasibility means that the finite horizon optimization problem in Section 3.2 is feasible at each triggering moment.

Theorem 2. *On the basis of DETM (10), the finite horizon optimization problem (18) is recursively feasible at the triggering moment k_i^d if the following conditions are satisfied:*

$$\theta_i\le\left(\frac{1}{N\left[\lambda_{\max}({A_i}^TA_i)\right]^{N-1}}\zeta_i\right)\|\chi_i\|^2, \tag{23}$$

$$\theta_i\le\frac{(1-{\alpha_i}^2){\eta_i}^2}{\lambda_{\max}(P_i)\left[\lambda_{\max}({A_i}^TA_i)\right]^{N-1}}, \tag{24}$$

$$\theta_i\le\frac{(1-{\alpha_i}^2){\eta_i}^2}{\lambda_{\max}(P_i)}, \tag{25}$$

$$\alpha_i\ge\sqrt{\frac{\lambda_{\max}\left(P_i\right)}{\lambda_{\min}\left(Q_i+{K_i}^TR_iK_i\right)+\lambda_{\max}\left(P_i\right)}}, \tag{26}$$

$$\alpha_i\ge\sqrt{\frac{\lambda_{\max}(P_i)}{N\lambda_{\min}(Q_i+{K_i}^TRK_i)+\lambda_{\max}(P_i)}}. \tag{27}$$

where

$$\theta_i=\theta_{i1}+\theta_{i2},$$

$$\theta_{i1}=\left[\lambda_{\max}\left({A_i}^TA_i\right)\right]^{N_a+1}\frac{\delta_{iM}\phi_i}{\lambda_{\min}\left(Q_{etm1}\right)},$$

$$\theta_{i2}=\frac{1-\left[\lambda_{\max}\left({A_i}^TA_i\right)\right]^{N_a}}{1-\lambda_{\max}\left({A_i}^TA_i\right)}\lambda_{\max}\left({C_i}^TC_i\right)\|W\|^2.$$

Proof. It is assumed that k_i^d is the current triggering moment and $\bar{k}_i^{d+1}$ is the next triggering time instant that satisfies the event-triggering condition (10). Then we can get

$$\left\|x_i\left(\bar{k}_i^{d+1}-1\right)-x_i^B\left(\bar{k}_i^{d+1}-1|k_i^d\right)\right\|_{Q_{etm1}}^2\le\delta_{iM}\phi_i \tag{28}$$

which implies

$$\left\| x_i\left(\bar{k}_i^{d+1}-1\right)-x_i^B\left(\bar{k}_i^{d+1}-1|k_i^d\right)\right\|^2 \le \frac{\delta_{iM}\phi_i}{\lambda_{\min}\left(Q_{etm1}\right)} \tag{29}$$

Next, consider the worst-case scenario where the ith vehicle suffers DoS attacks of maximum duration N_a at $\bar{k}_i^{d+1}$. The next triggering time instant in the worst-case scenario should be k_i^{d+1}, where $k_i^{d+1}=\bar{k}_i^{d+1}+N_a$. Thus, the error between the actual state and the predicted state of the ith vehicle in the worst-case scenario is

$$\begin{aligned} &x_i(k_i^{d+1})-x_i{}^*(k_i^{d+1}|k_i^d)\\ &\quad=x_i(\bar{k}_i^{d+1}+N_a)-x_i{}^*(\bar{k}_i^{d+1}+N_a|k_i^d)\\ &\quad=A_i{}^{N_a+1}\left[x_i(\bar{k}_i^{d+1}-1)-x_i{}^*(\bar{k}_i^{d+1}-1|k_i^d)\right]\\ &\qquad+A_i{}^{N_a}C_i\omega_i(\bar{k}_i^{d+1}-1)+\cdots+C_i\omega_i(\bar{k}_i^{d+1}+N_a-1) \end{aligned} \tag{30}$$

Thus, one can obtain that

$$\begin{aligned} \left\|x_i(k_i^{d+1})-x_i{}^*(k_i^{d+1}|k_i^d)\right\|^2 \le&\left[\lambda_{\max}\left(A_i{}^TA_i\right)\right]^{N_a+1}\frac{\delta_{iM}\phi_i}{\lambda_{\min}\left(Q_{etm1}\right)}\\ &+\sum_{m=0}^{N_a}\left(\|A_i\|^2\right)^m\|C_i\omega_i\|^2\\ \le&\theta_i \end{aligned} \tag{31}$$

The above θ_i is the upper bound on the error between the actual state and the predicted state at the next triggering instant. To ensure the recursive feasibility, it is essentially sufficient to show that the candidate state sequence generated by the candidate control input sequence at triggering moment k_i^{d+1} is feasible. Next, we discuss the two cases of k_i^{d+1}.

Case 1: $k_i^{d+1}\in\left(k_i^d,k_i^d+N\right]$

The error between the candidate state and predicted state can be written as

$$\bar{x}_i(k_i^{d+1}+t|k_i^{d+1})-x_i{}^*(k_i^{d+1}+t|k_i^d)=A_i{}^t\left[x_i(k_i^{d+1})-x_i{}^*(k_i^{d+1}|k_i^d)\right] \tag{32}$$

one can obtain that

$$\begin{aligned} &\left\|\bar{x}_i(k_i^{d+1}+t|k_i^{d+1})-x_i{}^*(k_i^{d+1}+t|k_i^d)\right\|^2\\ &\quad=\left\|\bar{e}_i(k_i^{d+1}+t|k_i^{d+1})-e_i{}^*(k_i^{d+1}+t|k_i^d)\right\|^2\\ &\quad\le\left[\lambda_{\max}(A_i{}^TA_i)\right]^t\left\|x_i(k_i^{d+1})-x_i{}^*(k_i^{d+1}|k_i^d)\right\|^2\\ &\quad\le\left[\lambda_{\max}(A_i{}^TA_i)\right]^t\theta_i \end{aligned} \tag{33}$$

By using the triangle inequality, it yields

$$\left\|\bar{e}_i(k_i^{d+1}+t|k_i^{d+1})\right\|^2\le\left\|e_i{}^*(k_i^{d+1}+t|k_i^d)\right\|^2+\left[\lambda_{\max}(A_i{}^TA_i)\right]^t\theta_i \tag{34}$$

When $t\in\left[0,N+k_i^d-k_i^{d+1}\right]$, due to the fact that θ_i satisfies condition (23), it can be obtained that

$$\begin{aligned} &\left\|\bar{e}_i(k_i^{d+1}+t|k_i^{d+1})\right\|^2\\ &\quad\le\left\|e_i{}^*(k_i^{d+1}+t|k_i^d)\right\|^2+\left[\lambda_{\max}(A_i{}^TA_i)\right]^t\theta_i\\ &\quad\le\left(1-\frac{k_i^{d+1}+t-k_i^d}{N}\zeta_i\right)\|\chi_i\|^2+\left[\lambda_{\max}(A_i{}^TA_i)\right]^t\theta_i\\ &\quad\le\left(1-\frac{t}{N}\zeta_i\right)\|\chi_i\|^2 \end{aligned} \tag{35}$$

Applying the similar derivation of (33), it leads to

$$\begin{aligned} &\left\|\bar{e}_i(k_i^d+N|k_i^{d+1})-e_i{}^*(k_i^d+N|k_i^d)\right\|^2\\ &\quad\le\left[\lambda_{\max}(A_i{}^TA_i)\right]^{k_i^d+N-k_i^{d+1}}\theta_i\\ &\quad\le\left[\lambda_{\max}(A_i{}^TA_i)\right]^{N-1}\theta_i \end{aligned} \tag{36}$$

By adopting matrix transformation scheme and triangle inequality, one has

$$\begin{aligned} &\left\|\bar{e}_i(k_i^d+N|k_i^{d+1})\right\|_{P_i}^2\\ &\quad\le\left\|e_i{}^*(k_i^d+N|k_i^d)\right\|_{P_i}^2+\lambda_{\max}(P_i)\left[\lambda_{\max}(A_i{}^TA_i)\right]^{N-1}\theta_i \end{aligned} \tag{37}$$

Since θ_i satisfies condition (24), the inequality (37) can be written as

$$\left\|\bar{e}_i(k_i^d+N|k_i^{d+1})\right\|_{P_i}^2\le\alpha_i{}^2\eta_i^2+(1-\alpha_i{}^2)\eta_i^2=\eta_i^2 \tag{38}$$

which implies $\left\|\bar{e}_i(k_i^d+N|k_i^{d+1})\right\|_{P_i}^2\le\eta_i{}^2$.

When $t\in\left[0,k_i^{d+1}-k_i^d\right)$, it follows from Assumption 3, we have

$$\begin{aligned} &\left\|\bar{e}_i(k_i^d+t+1+N|k_i^{d+1})\right\|_{P_i}^2-\left\|\bar{e}_i(k_i^d+t+N|k_i^{d+1})\right\|_{P_i}^2\\ &\quad\le-\left\|\bar{e}_i(k_i^d+t+N|k_i^{d+1})\right\|_{Q_i+K_i{}^TR_iK_i}^2 \end{aligned} \tag{39}$$

Summing the left and right sides of inequality (39) from $t=0$ to $t=k_i^{d+1}-k_i^d-1$, respectively, it yields

$$\left\|\bar{e}_i(k_i^{d+1}+N|k_i^{d+1})\right\|_{P_i}^2\le\frac{\lambda_{\max}(P_i)}{\lambda_{\min}(Q_i+K_i{}^TR_iK_i)+\lambda_{\max}(P_i)}\eta_i{}^2 \tag{40}$$

Based on the condition (26), one has

$$\left\|\bar{e}_i(k_i^{d+1}+N|k_i^{d+1})\right\|_{P_i}^2\le\alpha_i{}^2\eta_i^2 \tag{41}$$

Case 2: $k_i^{d+1}\in\left(k_i^d+N,k_i^d+N+N_a\right]$

The tracking error at the moment k_i^{d+1} satisfies the terminal constraint

$$\left\|e_i(k_i^{d+1})\right\|_{P_i}^2\le\left\|e_i{}^*(k_i^{d+1}|k_i^d)\right\|_{P_i}^2+\lambda_{\max}(P_i)\theta_i \tag{42}$$

Since θ_i satisfies condition (25), the inequality (42) can be written as

$$\left\|e_i(k_i^{d+1})\right\|_{P_i}^2\le\eta_i{}^2 \tag{43}$$

When $t\in[0,N-1)$, we have

$$\begin{aligned} &\left\|\bar{e}_i(k_i^{d+1}+t+1|k_i^{d+1})\right\|_{P_i}^2-\left\|\bar{e}_i(k_i^{d+1}+t|k_i^{d+1})\right\|_{P_i}^2\\ &\quad\le-\left\|\bar{e}_i(k_i^{d+1}+t|k_i^{d+1})\right\|_{Q_i+K_i{}^TR_iK_i}^2 \end{aligned} \tag{44}$$

Summing the left and right sides of inequality (44) from $t=0$ to $t=N-1$, respectively, it yields

$$\left\|\bar{e}_i(k_i^{d+1}+N|k_i^{d+1})\right\|_{P_i}^2-\left\|e_i(k_i^{d+1})\right\|_{P_i}^2\le-N\left\|\bar{e}_i(k_i^{d+1}+N|k_i^{d+1})\right\|_{Q_i+K_i{}^TR_iK_i}^2 \tag{45}$$

By adopting matrix transformation scheme, we have

$$\left\|\bar{e}_i(k_i^{d+1}+N|k_i^{d+1})\right\|_{P_i}^2\le\eta_i{}^2\frac{\lambda_{\max}(P_i)}{N\lambda_{\min}(Q_i+K_i{}^TRK_i)+\lambda_{\max}(P_i)} \tag{46}$$

According to the condition (27), one has

$$\left\|\bar{e}_i(k_i^{d+1}+N|k_i^{d+1})\right\|_{P_i}^2\le\alpha_i{}^2\eta_i{}^2 \tag{47}$$

From the above analysis, it can be demonstrated that the holding of conditions (23), (24), (25), (26), and (27) can ensure the recursive feasibility of the DETM-based DMPC algorithm proposed in this paper. This completes the proof.

4.2. Stability analysis

In this section, we are on the stage to investigate the stability of system (8) under DoS attacks.

Theorem 3. *The system (8) subjected to DoS attacks under our proposed DETM-based DMPC algorithm is ISPS if Theorem 2 holds.*

Proof. Selecting the optimal cost function at the triggering moment as the ISPS-Lyapunov function, so the ISPS-Lyapunov function for consecutive triggering moment can be expressed as $V_i^*(k_i^d) = J_i(x_i^*(k_i^d), u_i^*(k_i^d), X_i^a(k_i^d))$ and $V_i^*(k_i^{d+1}) = J_i(x_i^*(k_i^{d+1}), u_i^*(k_i^{d+1}), X_i^a(k_i^{d+1}))$. To facilitate the analysis of stability, define the candidate cost function obtained through the candidate state sequence and the candidate input sequence at moment k_i^{d+1} as $\bar{V}_i(k_i^{d+1}) = J_i(\bar{x}_i(k_i^{d+1}), \bar{u}_i(k_i^{d+1}), X_i^a(k_i^{d+1}))$. Considering that $V_i^*(k_i^{d+1})$ is the optimal cost function at moment k_i^{d+1}, it can be obtained that

$$V_i^*(k_i^{d+1}) - V_i^*(k_i^d) \leqslant \bar{V}_i(k_i^{d+1}) - V_i^*(k_i^d) \tag{48}$$

Define $\hat{V}_i(k_i^{d+1})$ as

$$\begin{aligned}\hat{V}_i(k_i^{d+1}) = &\sum_{t=0}^{N-1}\left[E_1(t) + \left\|u_i^*(k_i^{d+1}+t|k_i^d)\right\|_{R_i}^2\right] \\ &+ \sum_{t=0}^{N-1} E_2(t) + \left\|e_i^*(k_i^{d+1}+N|k_i^d)\right\|_{P_i}^2\end{aligned} \tag{49}$$

where

$$E_1(t) = \left\|x_i^*(k_i^{d+1}+t|k_i^d) - x_r(k_i^{d+1}+t) - d_{ir}\right\|_{Q_i}^2,$$

$$E_2(t) = \sum_{j\in\mathbb{C}_i}\left\|x_i^*(k_i^{d+1}+t|k_i^d) - x_j{}^B(k_i^{d+1}+t|k_i^d) - d_{ij}\right\|_{Q_{ij}}^2.$$

By subtracting and adding $\hat{V}_i(k_i^{d+1})$ in (48), one can obtain that

$$V_i^*(k_i^{d+1}) - V_i^*(k_i^d) \leqslant \bar{V}_i(k_i^{d+1}) - \hat{V}_i(k_i^{d+1}) + \hat{V}_i(k_i^{d+1}) - V_i^*(k_i^d) \tag{50}$$

Firstly, it follows from the first term $\bar{V}_i(k_i^{d+1}) - \hat{V}_i(k_i^{d+1})$ in inequality (50) that

$$\begin{aligned}\bar{V}_i(k_i^{d+1}) - \hat{V}_i(k_i^{d+1}) \leqslant &\sum_{t=0}^{N-1}\left[E_3(t) + E_4(t) + E_5(t)\right] \\ &+ \left\|\bar{x}_i(k_i^{d+1}+N|k_i^{d+1}) - x_i^*(k_i^{d+1}+N|k_i^d)\right\|_{P_i}^2\end{aligned} \tag{51}$$

where

$$E_3(t) = \left\|\bar{x}_i(k_i^{d+1}+t|k_i^{d+1}) - x_i^*(k_i^{d+1}+t|k_i^d)\right\|_{Q_i}^2,$$

$$E_4(t) = \sum_{j\in\mathbb{C}_i}\left\|\bar{x}_i(k_i^{d+1}+t|k_i^{d+1}) - x_i^*(k_i^{d+1}+t|k_i^d)\right\|_{Q_{ij}}^2,$$

$$E_5(t) = \sum_{j\in\mathbb{C}_i}\left\|x_j{}^B(k_i^{d+1}+t|k_i^{d+1}) - x_j{}^B(k_i^{d+1}+t|k_i^d)\right\|_{Q_{ij}}^2.$$

From (33), we have

$$\begin{aligned}&\left\|\bar{x}_i(k_i^{d+1}+t|k_i^{d+1}) - x_i^*(k_i^{d+1}+t|k_i^d)\right\|_{Q_i}^2 \\ &\quad\leqslant \lambda_{\max}(Q_i)\left[\lambda_{\max}(A_i{}^TA_i)\right]^t\theta_i\end{aligned} \tag{52}$$

Applying the similar derivation to the other terms in (51), one can obtain that

$$\begin{aligned}\bar{V}_i(k_i^{d+1}) - \hat{V}_i(k_i^{d+1}) \leqslant &\sum_{t=0}^{N-1}\lambda_{\max}(Q_i)\left[\lambda_{\max}(A_i{}^TA_i)\right]^t\theta_i \\ &+ \sum_{t=0}^{N-1}\lambda_{\max}(P_i)\left[\lambda_{\max}(A_i{}^TA_i)\right]^N\theta_i \\ &+ \sum_{t=0}^{N-1}\sum_{j\in\mathbb{C}_i}\left[\lambda_{\max}(Q_{ij})\left[\lambda_{\max}(A_i{}^TA_i)\right]^t\theta_i\right] \\ &+ \sum_{t=0}^{N-1}\sum_{j\in\mathbb{C}_i}\left[\lambda_{\max}(Q_{ij})\left[\lambda_{\max}(A_j{}^TA_j)\right]^t\theta_j\right] \\ \leqslant &(M_1+M_2+M_3)\theta_i + M_4\end{aligned} \tag{53}$$

where

$$M_1 = \frac{\lambda_{\max}(Q_i)\left[1-\left(\lambda_{\max}(A_i{}^TA_i)\right)^{N-1}\right]}{1-\lambda_{\max}(A_i{}^TA_i)},$$

$$M_2 = \lambda_{\max}(P_i)\left[\lambda_{\max}(A_i{}^TA_i)\right]^N,$$

$$M_3 = \sum_{j\in\mathbb{C}_i}\frac{\lambda_{\max}(Q_{ij})\left[1-\left(\lambda_{\max}(A_i{}^TA_i)\right)^{N-1}\right]}{1-\lambda_{\max}(A_i{}^TA_i)},$$

$$M_4 = \sum_{j\in\mathbb{C}_i}\frac{\lambda_{\max}(Q_{ij})\left[1-\left(\lambda_{\max}(A_j{}^TA_j)\right)^{N-1}\right]}{1-\lambda_{\max}(A_j{}^TA_j)}\theta_j.$$

Then it follows from the second term $\hat{V}_i(k_i^{d+1}) - V_i^*(k_i^d)$ in the right side of inequality (50) that

Case 1: $k_i^{d+1} \in \left(k_i^d, k_i^d + N\right]$

$$\begin{aligned}\hat{V}_i(k_i^{d+1}) - V_i^*(k_i^d) = &\sum_{t=k_i^d+N}^{k_i^{d+1}+N-1}\left[E_1(t|k_i^d) + \left\|u_i^*(t|k_i^d)\right\|_{R_i}^2 + E_2(t|k_i^d)\right] \\ &- \sum_{t=k_i^d}^{k_i^{d+1}-1}\left[E_1(t|k_i^d) + \left\|u_i^*(t|k_i^d)\right\|_{R_i}^2 + E_2(t|k_i^d)\right] \\ &+ \left\|e_i^*(k_i^{d+1}+N|k_i^d)\right\|_{P_i}^2 - \left\|e_i^*(k_i^d+N|k_i^d)\right\|_{P_i}^2\end{aligned} \tag{54}$$

Furthermore, we have

$$\begin{aligned}&\left\|e_i^*(k_i^{d+1}+N|k_i^d)\right\|_{P_i}^2 - \left\|e_i^*(k_i^d+N|k_i^d)\right\|_{P_i}^2 \\ &\quad\leqslant -\sum_{t=k_i^d+N}^{k_i^{d+1}+N-1}\left[\left\|e_i^*(t|k_i^d)\right\|_{Q_i}^2 + \left\|u_i^*(t|k_i^d)\right\|_{R_i}^2\right]\end{aligned} \tag{55}$$

By substituting (55) into (54), one gets

$$\begin{aligned}\hat{V}_i(k_i^{d+1}) - V_i^*(k_i^d) &\leqslant \sum_{t=k_i^d+N}^{k_i^{d+1}+N-1}\left[E_2(t)\right] - \left\|e_i(k_i^d)\right\|_{Q_i}^2 \\ &\leqslant -\lambda_{\min}(Q_i)\left\|e_i(k_i^d)\right\|^2 + M_5\end{aligned} \tag{56}$$

where $M_5 = N\sum_{j\in\mathbb{C}_i}\left[\frac{\lambda_{\max}(Q_{ij})}{\lambda_{\min}(P_i)}\alpha_i^2\eta_i^2 + \frac{\lambda_{\max}(Q_{ij})}{\lambda_{\min}(P_j)}\alpha_j^2\eta_j^2\right]$.

Case 2: $k_i^{d+1} \in \left(k_i^d + N, k_i^d + N + N_a\right]$

Applying the similar derivation in case 1, one can obtain that

$$\begin{aligned}\hat{V}_i(k_i^{d+1}) - V_i^*(k_i^d) = &\sum_{t=0}^{N-1}E_2(t) - \sum_{t=k_i^d-k_i^{d+1}+N}^{k_i^d-k_i^{d+1}+N-1}E_2(t) - \sum_{t=k_i^d-k_i^{d+1}+N}^{-1}E_2(t) \\ &- \sum_{t=0}^{N-1}\left[\left\|e_i^*(k_i^d+t|k_i^d)\right\|_{Q_i}^2 + \left\|u_i^*(k_i^d+t|k_i^d)\right\|_{R_i}^2\right] \\ &- \sum_{t=k_i^d+N}^{k_i^{d+1}-1}\left[\left\|e_i^*(t|k_i^d)\right\|_{Q_i}^2 + \left\|u_i^*(t|k_i^d)\right\|_{R_i}^2\right] \\ \leqslant &-\lambda_{\min}(Q_i)\left\|e_i(k_i^d)\right\|^2 + M_5\end{aligned} \tag{57}$$

Combining the inequalities (53), (56) and (57) yields

$$V_i^*(k_i^{d+1}) - V_i^*(k_i^d) \leqslant -\lambda_{\min}(Q_i)\left\|e_i(k_i^d)\right\|^2 + a\|W\|^2 + c \tag{58}$$

where

$$a = (M_1+M_2+M_3)M_7 + M_8,$$

$$c = (M_1+M_2+M_3)M_6 + M_9 + M_5,$$

$$M_6 = \left[\lambda_{\max}\left(A_i{}^TA_i\right)\right]^{N_a+1}\frac{\delta_{iM}\phi_i}{\lambda_{\min}\left(Q_{etm1}\right)},$$

$$M_7 = \frac{1-\left[\lambda_{\max}\left(A_i{}^TA_i\right)\right]^{N_a}}{1-\lambda_{\max}\left(A_i{}^TA_i\right)}\lambda_{\max}\left(C_i{}^TC_i\right),$$

$$M_8 = \sum_{j\in\mathbb{C}_i}\left[\frac{\lambda_{\max}(Q_{ij})\left[1-\left(\lambda_{\max}(A_j{}^TA_j)\right)^{N-1}\right]}{1-\lambda_{\max}(A_j{}^TA_j)}M_{8j}\right],$$

$$M_{8j} = \frac{1-\left[\lambda_{\max}\left(A_j{}^TA_j\right)\right]^{N_a}}{1-\lambda_{\max}\left(A_j{}^TA_j\right)}\lambda_{\max}\left(C_j{}^TC_j\right),$$

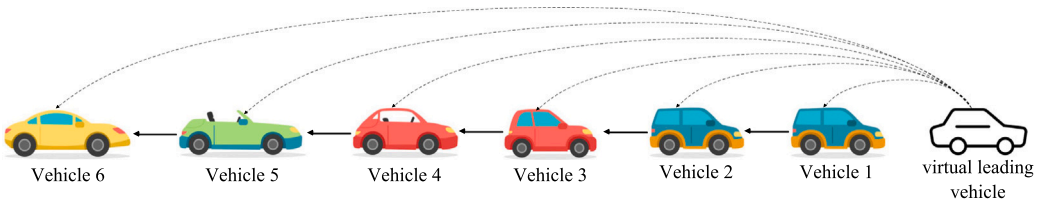
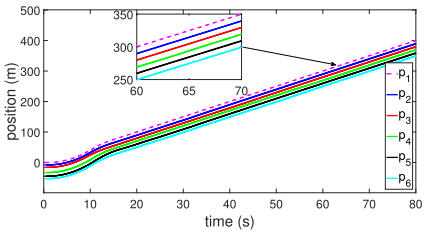
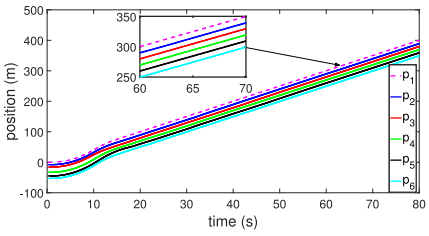


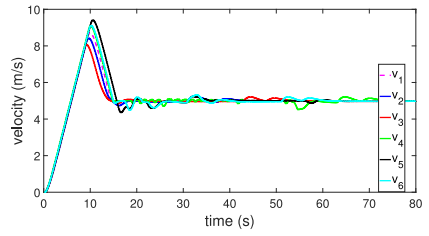
Fig. 2. Network topology.



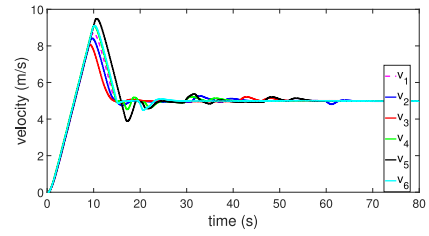
(a) Position trajectories, $\Psi_{\max} = 67$.



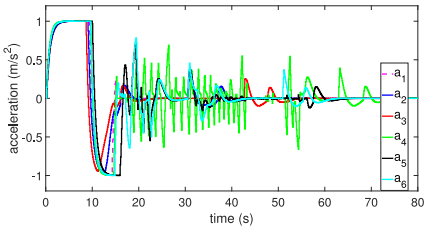
(b) Position trajectories, $\Psi_{\max} = 178$.



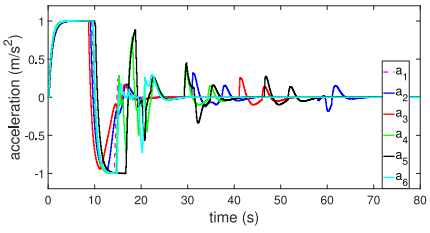
(c) Velocity trajectories, $\Psi_{\max} = 67$.



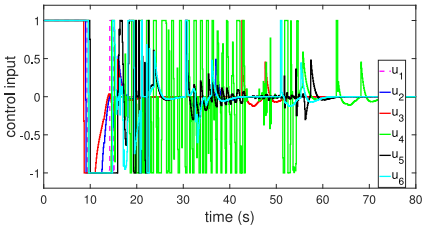
(d) Velocity trajectories, $\Psi_{\max} = 178$.



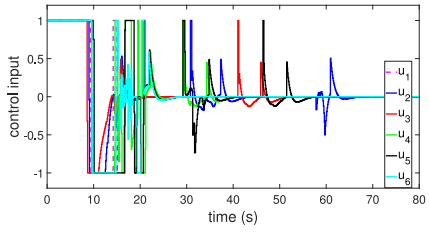
(e) Acceleration trajectories, $\Psi_{\max} = 67$.



(f) Acceleration trajectories, $\Psi_{\max} = 178$.



(g) Control input trajectories, $\Psi_{\max} = 67$.



(h) Control input trajectories, $\Psi_{\max} = 178$.

Fig. 3. The trajectories of states and control inputs.

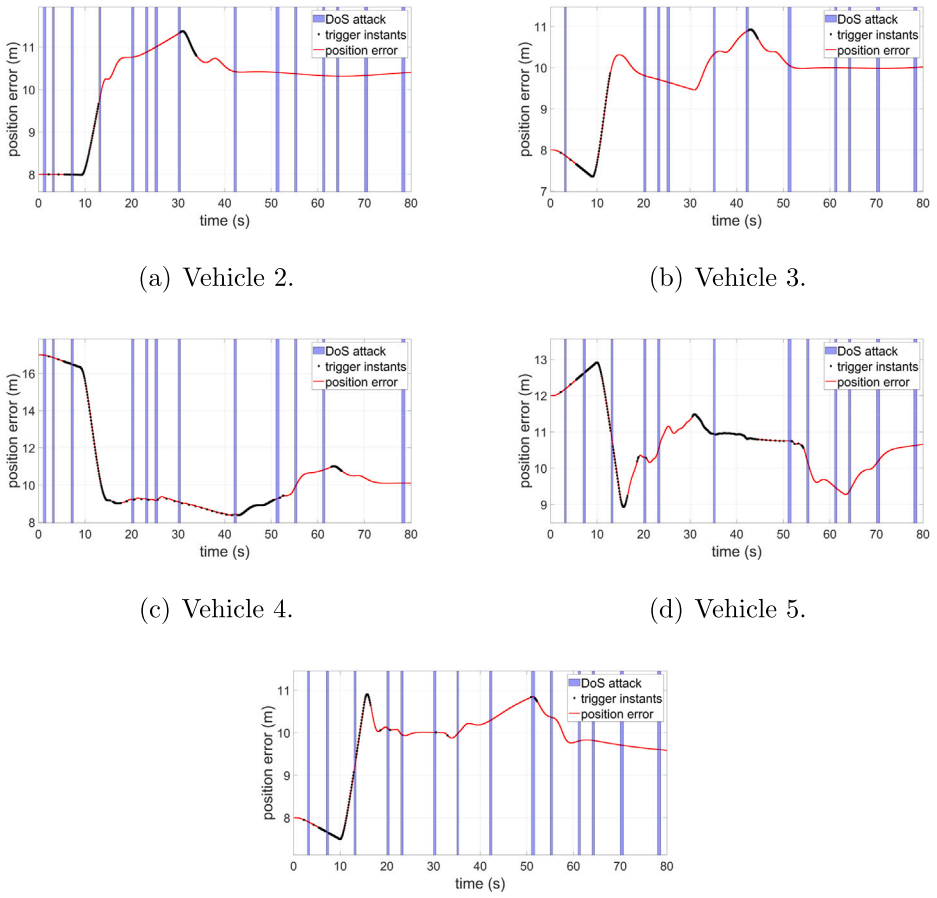
$$M_9 = \sum_{j\in\mathbb{C}_i}\left[\frac{\lambda_{\max}(Q_{ij})\left[1-\left(\lambda_{\max}(A_j{}^TA_j)\right)^{N-1}\right]}{1-\lambda_{\max}(A_j{}^TA_j)}M_{9j}\right],$$

$$M_{9j} = \left[\lambda_{\max}\left(A_j{}^TA_j\right)\right]^{N_a+1}\frac{\delta_{jM}\phi_j}{\lambda_{\min}\left(Q_{etm1}\right)}.$$

From Definition 1 and inequality (58), it can be obtained that the closed-loop system (8) is ISPS. The proof is completed.

5. Simulation

In this section, the main results of this paper are illustrated using numerical simulations performed via MATLAB.



(a) Vehicle 2. (b) Vehicle 3.

(c) Vehicle 4. (d) Vehicle 5.

(e) Vehicle 6.

Fig. 4. The position error trajectories under DoS attacks when $\Psi_{\max} = 67$.

Table 1
Vehicle Parameters.

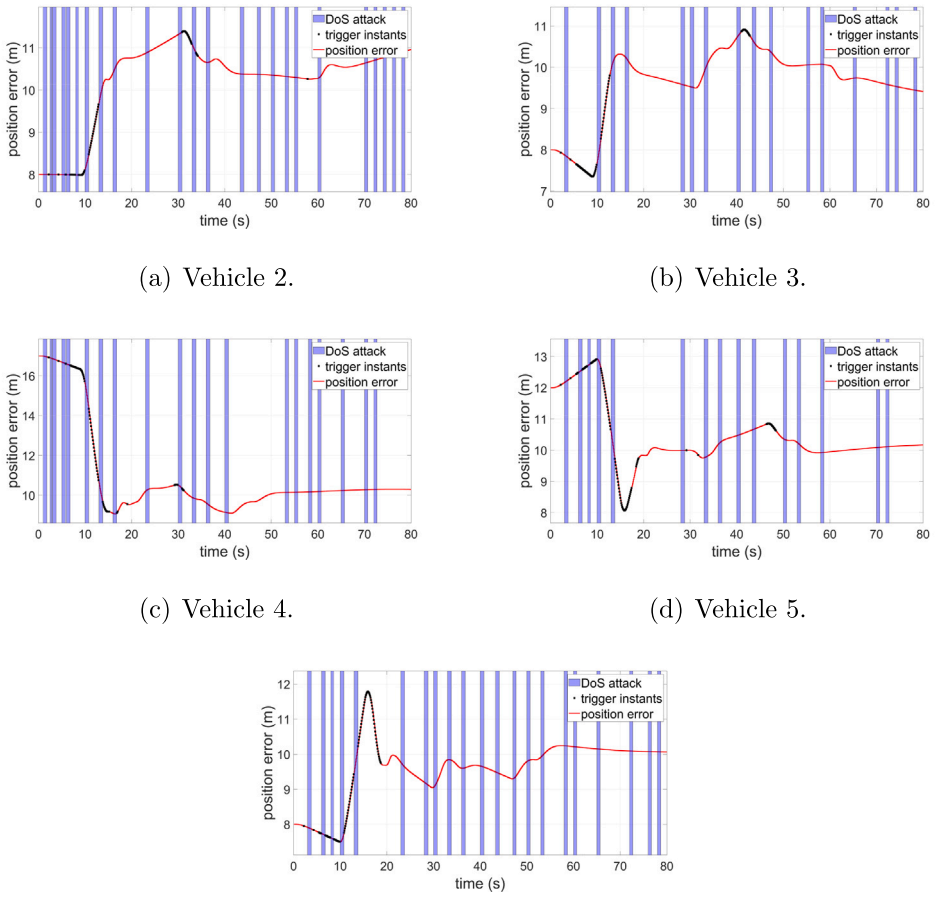
Vehicle	τ_i	$\omega_i(k)$	K_i
Vehicle 1	0.83	$0.008\sin(0.17k)$	$[-0.91 \quad -2.34 \quad -1.42]$
Vehicle 2	0.83	$0.008\sin(0.17k)$	$[-0.91 \quad -2.34 \quad -1.42]$
Vehicle 3	0.74	$0.009\sin(0.16k)$	$[-0.91 \quad -2.29 \quad -1.31]$
Vehicle 4	0.65	$0.006\sin(0.17k)$	$[-0.91 \quad -2.24 \quad -1.20]$
Vehicle 5	0.76	$0.007\sin(0.18k)$	$[-0.91 \quad -2.30 \quad -1.33]$
Vehicle 6	0.70	$0.008\sin(0.17k)$	$[-0.91 \quad -2.27 \quad -1.26]$

5.1. Parameter configuration

It is assumed that the CVP system has a virtual leading vehicle, a leading vehicle, and five following vehicles. The communication topology among the vehicles is shown in Fig. 2. The sampling period is set as $\Delta T = 0.1s$. For the DoS attacks parameters, we set $N_a = 7$. The longitudinal dynamics parameters of vehicle are choose as in [42]. In this paper, the external disturbance is assumed to be bounded, and a sinusoidal function is introduced to model the external disturbance. The engine inertia time constant, external disturbance and state feedback law for each vehicle are shown in Table 1. For the ith vehicle in the CVP system, the corresponding matrix P_i can be obtained by computing the discrete Riccati equation in Remark 3. We choose the parameters $\varsigma_i = 0.9$, $\alpha_i{}^2 = 0.99$, $\eta_i{}^2 = 9.6$, $\delta_{iM} = 2$, $\delta_{im} = 0.5$, and $\phi_i = 0.0022$. The weighting matrices are set as $Q_i = I$, $Q_{ij} = I$, $Q_{etm1} = 0.01I$, and $Q_{etm2} = I$. Considering the security and passenger comfort, the constraints imposed on each vehicle are set as $-1 \leqslant u_i \leqslant 1$, $0(\mathrm{m/s}) \leqslant v_i \leqslant 15(\mathrm{m/s})$, and $-3.5(\mathrm{m/s^2}) \leqslant a_i \leqslant 3.5(\mathrm{m/s^2})$. Assuming that the virtual leading vehicle has an initial position of 0 and travels at a constant speed of 5 m/s, the ideal vehicle spacing is $d = 10$ m. The initial state of each vehicle is set to $x_1(0) = [0;0;0]$, $x_2(0) = [-8;0;0]$, $x_3(0) = [-16;0;0]$, $x_4(0) = [-33;0;0]$, $x_5(0) = [-45;0;0]$, and $x_6(0) = [-53;0;0]$, respectively.

5.2. Platoon control under different DoS attacks durations

In order to verify the effectiveness of the proposed algorithm, the control of CVP system under different DoS attacks durations is simulated. In simulation, the DoS attacks durations are set to be $\Psi_{\max} = 67$ and $\Psi_{\max} = 178$, respectively. The state trajectories of each vehicle when $\Psi_{\max} = 67$ and $\Psi_{\max} = 178$ are shown in Fig. 3. Under two different DoS attack durations, it can be seen that all vehicles can reach the desired spacing, and achieve the same speed and acceleration as the virtual leader vehicle. The control inputs for all vehicles satisfy the input constraints. For the 2-nd to 6-th following vehicle, the position error $\Delta p_i(k)$ is defined as $\Delta p_i(k) = p_{i-1}(k) - p_i(k), i \in [2,6]$. The position error, DoS attacks sequence and event-triggering sequence for each vehicle when $\Psi_{\max} = 67$ and $\Psi_{\max} = 178$ are shown in Fig. 4 and Fig. 5, respectively. We can see that the DETM can handle DoS attacks by reducing transmission frequency. The simulation results show that the proposed DETM-based DMPC algorithm can effectively deal with the cooperative control of CVP system under different DoS attack durations.



(a) Vehicle 2. (b) Vehicle 3.

(c) Vehicle 4. (d) Vehicle 5.

(e) Vehicle 6.

Fig. 5. The position error trajectories under DoS attacks when $\Psi_{\max} = 178$.

5.3. Platoon control under different control algorithms

In order to better demonstrate the performance of algorithm proposed in this paper, we compare it with the algorithm in [42] under the same DoS attacks sequence when $\Psi_{\max} = 67$. The evaluation method in [41] is used to quantitatively assess the effectiveness of the proposed algorithm in terms of resilient control performance and communication scheduling. First, the average triggering rate F_{ave} in the time interval $[0, T_{end}]$ is defined as

$$F_{ave} = \frac{1}{\mathcal{N}-1}\sum_{i=2}^{\mathcal{N}}\left(\frac{1}{T_{end}}\sum_{k=0}^{T_{end}}\mathcal{O}_{ik}\right)\cdot 100\%$$

where

$$\mathcal{O}_{ik} = \begin{cases} 1, & \text{DTEM condition is satisfied at instant } k \\ 0, & \text{otherwise} \end{cases}$$

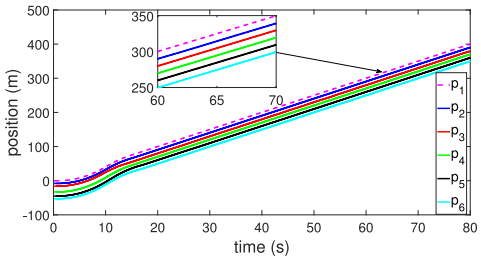
Then, the average position error e_{ave} in the time interval $[0, T_{end}]$ is defined as

$$e_{ave} = \frac{1}{\mathcal{N}-1}\sum_{i=2}^{\mathcal{N}}\left(\frac{1}{T_{end}}\sum_{k=0}^{T_{end}} p_{i-1}(k) - p_i(k) - d\right)$$

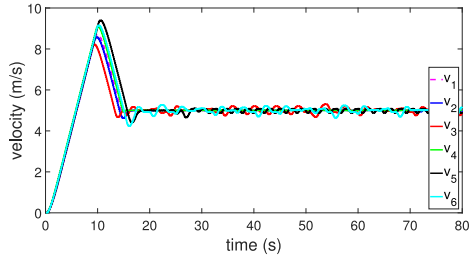
By calculating the data in the simulation, the average triggering rate and the average position error under our proposed algorithm are calculated as $F_{ave} = 0.206$ and $e_{ave} = 0.876$. The state trajectories and control input trajectories of the comparison simulation are shown in Fig. 6. The average triggering rate and the average position error in the comparison simulation are calculated as $F_{ave} = 0.386$ and $e_{ave} = 0.805$. It can be obtained that the comparison simulation have a lower average position error rate and a more significant average triggering rate. Our proposed algorithm reduces the number of triggers by 46.6% in the time interval $[0, 800]$. It is shown through simulation results that our proposed algorithm has effective control performance on the CVP system under DoS attacks and can effectively reduce the number of event triggers.

6. Conclusion

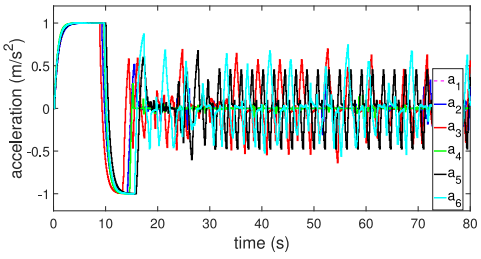
The DETM-based DMPC algorithm for heterogeneous CVP system under DoS attacks has been investigated in this paper. Firstly, a DETM was designed to reduce the frequency of data exchange between vehicles in the CVP system. Then, robust constraint was designed in the DMPC algorithm to deal with uncertainties in CVP systems. Whereafter, a packet replenishment mechanism was designed to ensure the integrity and effectiveness of information interaction. Sufficient conditions were given to guarantee the recursive feasibility of the DETM-based DMPC algorithm, and it was shown that the CVP system under this algorithm is ISPS under DoS attacks and external disturbance. Finally, the effectiveness of the algorithm was verified by numerical simulation based on MATLAB. However, the drawback of the control strategy in this paper is that it does not consider the impact of time-varying spacing policy and time-delays. In our future work, physical failure of motors in connected vehicles [51] should be considered together with the cyber attacks, which can provide the unified security of connected vehicles.



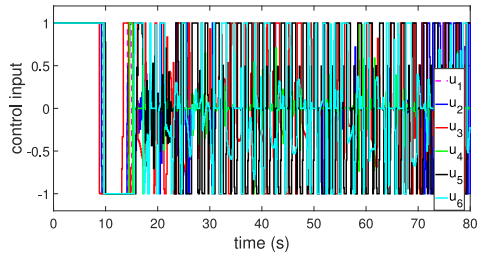
(a) Position trajectories.



(b) Velocity trajectories.



(c) Acceleration trajectories.



(d) Control input trajectories.

Fig. 6. The comparative simulation when $\Psi_{\max} = 67$.

CRediT authorship contribution statement

Hao Zeng: Writing – original draft, Investigation. **Zehua Ye:** Methodology. **Dan Zhang:** Writing – review & editing, Supervision, Funding acquisition, Conceptualization.

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.

Acknowledgments

This work was partially supported by the National Natural Science Foundation of China under Grant No. 62322315 and No. 61873237, the Zhejiang Provincial Natural Science Foundation of China under Grant No. LR22F030003.

References

[1] Ren R, Li H, Han T, Tian C, Zhang C, Zhang J, et al. Vehicle crash simulations for safety: Introduction of connected and automated vehicles on the roadways. Accid Anal Prev 2023;186:107021.
[2] Yang F, Gu Z, Hua L, Yan S. A resource-aware control approach to vehicle platoons under false data injection attacks. ISA Trans 2022;131:367–76.
[3] Mousavinejad E, Vlacic L. Secure platooning control of automated vehicles under cyber attacks. ISA Trans 2022;127:229–38.
[4] Liu Y, Yao D, Li H, Lu R. Distributed cooperative compound tracking control for a platoon of vehicles with adaptive NN. IEEE Trans Cybern 2022;52(7):7039–48.
[5] Chen M, Yan M. How to protect smart and autonomous vehicles from stealth viruses and worms. ISA Trans 2023;141:52–8.
[6] Parkinson S, Ward P, Wilson K, Miller J. Cyber threats facing autonomous and connected vehicles: Future challenges. IEEE Trans Intell Transp Syst 2017;18(11):2898–915.
[7] Wu C, Pan W, Staa R, Liu J, Sun G, Wu L. Deep reinforcement learning control approach to mitigating actuator attacks. Automatica 2023;152:110999.
[8] Cheng J, Wu Y, Wu Z-G, Yan H. Nonstationary filtering for fuzzy Markov switching affine systems with quantization effects and deception attacks. IEEE Trans Syst Man Cybern: Syst 2022;52(10):6545–54.
[9] Cheng J, Wang Y, Park JH, Cao J, Shi K. Static output feedback quantized control for fuzzy Markovian switching singularly perturbed systems with deception attacks. IEEE Trans Fuzzy Syst 2022;30(4):1036–47.
[10] Cheng J, Huang W, Park JH, Cao J. A hierarchical structure approach to finite-time filter design for fuzzy Markov switching systems with deception attacks. IEEE Trans Cybern 2022;52(8):7254–64.
[11] Xie M, Ding D, Ge X, Han Q-L, Dong H, Song Y. Distributed platooning control of automated vehicles subject to replay attacks based on proportional integral observers. IEEE/CAA J Autom Sin 2022;1–13.
[12] Xu X, Li X, Dong P, Liu Y, Zhang H. Robust reset speed synchronization control for an integrated motor-transmission powertrain system of a connected vehicle under a replay attack. IEEE Trans Veh Technol 2021;70(6):5524–36.
[13] Chen P, Zhang D, Yu L, Yan H. Dynamic event-triggered output feedback control for load frequency control in power systems with multiple cyber attacks. IEEE Trans Syst Man Cybern: Syst 2022;52(10):6246–58.
[14] Zhang D, Ye Z, Feng G, Li H. Intelligent event-based fuzzy dynamic positioning control of nonlinear unmanned marine vehicles under DoS attack. IEEE Trans Cybern 2022;52(12):13486–99.
[15] Mokari H, Firouzmand E, Sharifi I, Doustmohammadi A. Resilient control strategy and attack detection on platooning of smart vehicles under DoS attack. ISA Trans 2024;144:51–60.
[16] Ngo V-T, Liu Y-C. Distributed consensus control of networked robotic systems with dynamic leader under time-varying delays and Denial-of-Service attacks. IEEE Access 2022;10:92663–72.
[17] Ye Z, Zhang D, Feng G, Yan H. Finite-time consensus of leader-following MASs under DoS attacks. IEEE Control Syst Lett 2023;7:3409–14.
[18] Yang H, Ju S, Xia Y, Zhang J. Predictive cloud control for networked multiagent systems with quantized signals under DoS attacks. IEEE Trans Syst Man Cybern: Syst 2021;51(2):1345–53.
[19] Guo X-G, Liu P-M, Wu Z-G, Zhang D, Ahn CK. Hybrid event-triggered group consensus control for heterogeneous multiagent systems with tvnud faults and stochastic FDI attacks. IEEE Trans Autom Control 2023;68(12):8013–20.
[20] Abdollahi Biron Z, Dey S, Pisu P. Real-time detection and estimation of Denial of Service attack in connected vehicle systems. IEEE Trans Intell Transp Syst 2018;19(12):3893–902.
[21] Zhao N, Zhao X, Xu N, Zhang L. Resilient event-triggered control of connected automated vehicles under cyber attacks. IEEE/CAA J Autom Sin 2023;10(12):2300–2.
[22] Ge X, Han Q-L, Wu Q, Zhang X-M. Resilient and safe platooning control of connected automated vehicles against intermittent Denial-of-Service attacks. IEEE/CAA J Autom Sin 2023;10(5):1234–51.
[23] Li Z, Zhao H, Wang Y, Ren Y, Chen Z, Chen C. Adaptive event-triggered control for almost sure stability for vehicle platooning under interference and stochastic attacks. ISA Trans 2023;138:120–32.
[24] Zhang D, Shen Y-P, Zhou S-Q, Dong X-W, Yu L. Distributed secure platoon control of connected vehicles subject to DoS attack: Theory and application. IEEE Trans Syst Man Cybern: Syst 2021;51(11):7269–78.
[25] Merco R, Ferrante F, Pisu P. A hybrid controller for DoS-resilient string-stable vehicle platoons. IEEE Trans Intell Transp Syst 2021;22(3):1697–707.

[26] Tan G, Ren H, Zhang B, Deng F. Event-triggered control strategy based on absolute velocity and relative position measurements for second-order nonlinear multi-agent systems under DoS attacks. Neurocomputing 2024;574:127239.
[27] Lv G, Peng Z, Li Y, Liu L, Wang D. Barrier-certified model predictive cooperative path following control of connected autonomous surface vehicles. IEEE Trans Netw Sci Eng 2023;10(6):3354–67.
[28] Kennedy JM, Heinovski J, Quevedo DE, Dressler F. Centralized model predictive control with human-driver interaction for platooning. IEEE Trans Veh Technol 2023;72(10):12664–80.
[29] Feng S, Sun H, Zhang Y, Zheng J, Liu HX, Li L. Tube-based discrete controller design for vehicle platoons subject to disturbances and saturation constraints. IEEE Trans Control Syst Technol 2020;28(3):1066–73.
[30] Li Z, Xu H, Lin Z, Dong L, Chen Y. Event-triggered robust distributed output feedback model predictive control for nonlinear MASs against false data injection attacks. ISA Trans 2023;141:197–211.
[31] R. R, S.J. M, Jacob J. Dynamic consensus of linear multi-agent system using self-triggered distributed model predictive control. ISA Trans 2023;142:177–87.
[32] Chen J, Wei H, Zhang H, Shi Y. Asynchronous self-triggered stochastic distributed MPC for cooperative vehicle platooning over vehicular ad-hoc networks. IEEE Trans Veh Technol 2023;72(11):14061–73.
[33] Ju Z, Zhang H, Tan Y. Distributed stochastic model predictive control for heterogeneous vehicle platoons subject to modeling uncertainties. IEEE Intell Transp Syst Mag 2022;14(2):25–40.
[34] Ding B, Ge L, Pan H, Wang P. Distributed mpc for tracking and formation of homogeneous multi-agent system with time-varying communication topology. Asian J Control 2016;18(3):1030–41.
[35] Chen L, Zhan J, Zhang L. Distributed model predictive control of vehicle platoons under switching communication topologies. IMA J Math Control Inform 2023;dnad023.
[36] Zhu P, Jin S, Bu X, Hou Z. Distributed data-driven event-triggered fault-tolerant control for a connected heterogeneous vehicle platoon with sensor faults. IEEE Trans Intell Transp Syst 2023;1–12.
[37] Liu J, Wu L, Wu C, Luo W, Franquelo LG. Event-triggering dissipative control of switched stochastic systems via sliding mode. Automatica 2019;103:261–73.
[38] Yu T, Zhao Y, Wang J, Liu J. Event-triggered sliding mode control for switched genetic regulatory networks with persistent dwell time. Nonlinear Anal Hybrid Syst 2022;44:101135.
[39] Ye Z, Zhang D, Wu Z-G, Yan H. A3C-based intelligent event-triggering control of networked nonlinear unmanned marine vehicles subject to hybrid attacks. IEEE Trans Intell Transp Syst 2022;23(8):12921–34.
[40] Wen S, Guo G, Chen B, Gao X. Event-triggered cooperative control of vehicle platoons in vehicular ad hoc networks. Inform Sci 2018;459:341–53.
[41] Ge X, Xiao S, Han Q-L, Zhang X-M, Ding D. Dynamic event-triggered scheduling and platooning control co-design for automated vehicles over vehicular ad-hoc networks. IEEE/CAA J Autom Sin 2022;9(1):31–46.
[42] Chen J, Zhang H, Yin G. Distributed dynamic event-triggered secure model predictive control of vehicle platoon against DoS attacks. IEEE Trans Veh Technol 2023;72(3):2863–77.
[43] Zheng Y, Li SE, Li K, Ren W. Platooning of connected vehicles with undirected topologies: Robustness analysis and distributed h-infinity controller synthesis. IEEE Trans Intell Transp Syst 2018;19(5):1353–64.
[44] Wu C, Wu L, Liu J, Jiang Z-P. Active defense-based resilient sliding mode control under Denial-of-Service attacks. IEEE Trans Inf Forensics Secur 2020;15:237–49.
[45] Ye Z, Zhang D, Wu Z-G. Adaptive event-based tracking control of unmanned marine vehicle systems with DoS attack. J Franklin Inst 2021;358(3):1915–39.
[46] De Persis C, Tesi P. Input-to-state stabilizing control under Denial-Of-Service. IEEE Trans Autom Control 2015;60(11):2930–44.
[47] Ye Z, Zhang D, Deng C, Yan H, Feng G. Finite-time resilient sliding mode control of nonlinear UMV systems subject to DoS attacks. Automatica 2023;156:111170.
[48] Ni H, Xu Z, Cheng J, Zhang D. Robust stochastic sampled-data-based output consensus of heterogeneous multi-agent systems subject to random DoS attack: A Markovian jumping system approach. Int J Control Autom Syst 2019;17:1687–98.
[49] Dai Y, Li M, Zhang K, Shi Y. Robust and resilient distributed mpc for cyber-physical systems against DoS attacks. IEEE Trans Ind Cyber-Phys Syst 2023;1:44–55.
[50] Sun Q, Chen J, Shi Y. Event-triggered robust mpc of nonlinear cyber-physical systems against DoS attacks. Sci China Inf Sci 2022;65(1):110202.
[51] Chen Y, Zhang D, Yan R. Domain adaptation networks with parameter-free adaptively rectified linear units for fault diagnosis under variable operating conditions. IEEE Trans Neural Netw Learn Syst 2023;1–14.