Intelligence & Robotics

Research Article

Open Access

Robust distributed model predictive control of connected vehicle platoon against DoS attacks

Hao Zeng[1], Zehua Ye[1], Dan Zhang[1], Qun Lu[2]

[1]College of Information Engineering, Zhejiang University of Technology, Hangzhou 310014, Zhejiang, China.
[2]The School of Aeronautical Engineering, Taizhou University, Jiaojiang 318000, Zhejiang, China.

Correspondence to: Dr. Zehua Ye, College of Information Engineering, Zhejiang University of Technology, No.288 Liuhe Road, Hangzhou 310014, Zhejiang, China. E-mail: 2111803109@zjut.edu.cn

How to cite this article: Zeng H, Ye Z, Zhang D, Lu Q. Robust distributed model predictive control of connected vehicle platoon against DoS attacks. *Intell Robot* 2023;3(3):288-305. http://dx.doi.org/10.20517/ir.2023.19

Received: 15 Mar 2023 **First Decision:** 9 May 2023 **Revised:** 31 May 2023 **Accepted:** 27 Jun 2023 **Published:** 25 Jul 2023

Academic Editors: Simon X. Yang, Hongtian Chen **Copy Editor:** Yanbin Bai **Production Editor:** Yanbin Bai

Abstract

This paper investigates the robust distributed model predictive control (DMPC) of connected vehicle platoon (CVP) systems subject to denial-of-service (DoS) attacks. The main objective is to design a DMPC algorithm that enables the CVP system to achieve exponential tracking performance. First, a switched system model is proposed for the networked CVP system in the presence of DoS attacks. Then the sufficient conditions for the exponential stability of tracking the performance of the CVP control system under DoS attacks are obtained by constructing a specific Lyapunov function and using the topological matrix decoupling technique. In our paper, the DoS attack phenomenon is handled by introducing the frequency and duration parameters, and a quantitative relationship between the exponential decay rate of the CVP system and the DoS attacks parameters is established based on the conditions proposed in the system design, and the critical value of the DoS attack duration ratio is also derived. Finally, the effectiveness of the proposed algorithm is verified through a simulation of a CVP system consisting of one leading vehicle and three following vehicles.

Keywords: Distributed model predictive control (DMPC), connected vehicle platoon (CVP), denial-of-service (DoS) attacks, switched system, linear matrix inequalities (LMIs)

1. INTRODUCTION

In recent decades, the number of traffic congestions and traffic accidents has significantly increased due to the rapid growth in the number of vehicles. It has shown that by controlling the spacing among vehicles in connected vehicle platoons (CVPs), the air resistance of following vehicles during travel could be reduced, effectively reducing fuel consumption[1]. Moreover, by sharing the state information of surrounding vehicles in CVPs, the vehicles can be coordinated to achieve the desired trajectory and thus improve the efficiency and safety of road traffic[2,3]. As a result, the cooperative control of intelligent CVPs has received considerable attention.

Intelligent connected vehicles are typical complex cyber-physical systems (CPS) with deep integration of multiple systems, such as automotive systems, traffic rules, information systems, and communication networks. As intelligent connected vehicles combine various critical infrastructures through heterogeneous networks, cyber-attacks on intelligent connected vehicles are becoming more prominent due to the growing openness of networks[4,5]. Existing cyber-attacks can be broadly classified into denial-of-service (DoS) attacks[6–8], replay attacks[9], and deception attacks[10–12]. Among them, DoS attacks are the most common form of cyber-attacks and, therefore, receive much attention in current research[13]. When DoS attacks occur, many illegal request services are sent within a certain period, which causes the CPU and memory of the server to rise so that the system cannot handle the normal request services sent by legitimate users[14,15]. There have been some research results reported on DoS attacks. In Ref.[16], a scheme that can detect the occurrence of DoS attacks in real time was designed, and the impact of DoS attacks on CVP systems was evaluated. In Ref.[17], the finite-time stability of networked control systems in the presence of DoS attacks was investigated, and the number of data transmissions was reduced by using the event-triggered method. In Ref.[18], a resilient control strategy for CVP systems under DoS attacks was proposed and demonstrated to enable cooperative control of vehicles. In Ref.[19], the DoS attacks were considered as a continuous packet loss, and a resilient controller was proposed for CVPs under DoS attacks, and the effectiveness of the controller was demonstrated. In Ref.[20], a networked interconnection system under DoS attacks was studied, and sufficient conditions of the exponential stability for the system were obtained by using the average dwell time approach. In Ref.[21], a controller was designed for a CVP control system under DoS attacks using a switched system approach, and the feasibility of the results was verified by simulation and experimentation. The occurrence of DoS attacks in CVP control systems can block the data transmission in the communication channel, which can degrade the performance of CVPs and even lead to collisions among vehicles[22,23]. Thus, we will focus on the security control issues caused by DoS attacks in the CVP system in this paper. Although the above results are very effective in solving some typical cyber-attacks, they do not consider the problem of constraints such as the input and state. Thus, the above results cannot be applied to such CVP systems as those parameters of the connected vehicles are generally constrained.

The design of Model Predictive Control (MPC) algorithms has been extensively investigated in order to better solve the constraint problem in control[24]. Nowadays, the research on MPC can be mainly classified into centralized model predictive control[25] and distributed model predictive control (DMPC)[26,27]. Centralized model predictive control has good optimization capabilities but is usually computationally burdensome if it is used for large-scale systems. In recent years, the DMPC has received increasing attention as it is suitable to solve the large-scale system control problem due to its excellent control performance, ability to handle constraints, and flexible structure. In large-scale systems, such as CVPs, it is difficult to use centralized model predictive control because vehicles cannot receive global information from each other. Therefore, DMPC has been extensively investigated in the field of CVP control systems. In Ref.[26], a DMPC algorithm was proposed for an intelligent CVP system with nonlinear dynamics and unidirectional communication topology, which considers the constraint problem of the system while ensuring the asymptotic stability of the CVP system. In Ref.[27], a DMPC approach was used to solve the input and state constraint problem and finally to achieve the desired tracking problem for a multi-intelligent system. In Ref.[28], a dual-mode DMPC algorithm was proposed and demonstrated through simulation to significantly reduce the computational burden. Also, there are some studies on the DMPC of CVP systems under DoS attacks[29–31]. In Ref.[29], a secure DMPC control algorithm was proposed in order to make the CVP system eventually stable under DoS attacks, and the effectiveness of the algorithm was demonstrated by simulation. In Ref.[31], a DMPC algorithm based on a dynamic event-triggered method was proposed for CVP systems under DoS attacks, which reduces the amount of data computation by using the dynamic event-triggered method on the basis of ensuring the stability of the CVP system in the end. Although the above results can well solve the stabilization problem of the CVP system in the presence of DoS attacks, the issue of how the DoS attacks affect system performance has not been well investigated yet. Therefore, the motivation of this work is to study the security control problem of the CVP system under DoS attacks, and our attention is focused on the derivation of the quantitative relationship between system performance and DoS attacks.

Based on the above discussion, this work is concerned with the DMPC of CVP systems under DoS attacks. The main objective is to investigate how the DoS attacks affect the performance of the CVP system and obtain sufficient conditions to guarantee the exponential stability of the tracking error of the CVP system under DoS attacks. It is assumed that all communication channels of the CVP system are jammed when DoS attacks occur and then models the closed-loop CVP system under DoS attacks as a switched system. A robust DMPC algorithm is proposed to enable the CVP system to handle optimization problems with input constraints well while ensuring the exponential stability of the tracking error. In the part of the simulation, the effectiveness of our proposed algorithm is demonstrated through numerical simulations. The main contributions of this paper are summarized as follows.

(1) A robust DMPC algorithm is proposed to achieve resilient cooperative control of CVP systems under DoS attacks.

(2) Sufficient conditions for the exponential stability of the tracking error of the CVP system under DoS attacks are derived based on the switched system approach. A quantitative relationship between the exponential decay rate and the frequency and duration of DoS attacks is established. The critical value of the DoS attack duration ratio (DADR) is also derived.

Notations: In this paper, R denotes the sets of real numbers, $R^{n\times n}$denotes the sets of $n \times n$ real matrices, and $R^{m\times n}$denotes $m \times n$ real matrix. We let $\mathcal{N}$ denote the set of natural numbers and define $\mathcal{N}^+ = \mathcal{N} \cap \{0\}$. Let I_n denote the n-dimensional identity matrix and $\otimes$ denote the Kronecker product.

2. PRELIMINARIES AND PROBLEM FORMULATION

This section includes four main parts: communication graph, vehicle model, DoS attacks, and problem description. The structure of a CVP control system is shown in Figure 1. The position, velocity, and acceleration of the vehicles are sampled at each sampling moment and are transmitted according to the pre-designed communication topology. The communication channel is blocked when DoS attacks occur.

2.1. Communication graph

Considering that there is one leading vehicle and N following vehicles. We represent the communication interactions among vehicles by using an undirected communication graph[32]. For the graph ξ, the adjacency matrix $\mathcal{A}_N$ is defined as $\mathcal{A}_N = [a_{ij}] \in R^{N\times N}$ $(i, j = 1, ..., N)$, $a_{ij} = 0$ denotes the i-th following vehicle cannot obtain communication from the j-th following vehicle; otherwise, $a_{ij} = 1$. It is assumed that $a_{ii} = 0$. The Laplace matrix is defined as $\mathcal{L}_{\mathrm{N}} = [l_{ij}] \in R^{N\times N}$ $(i, j = 1, ..., N)$, where $l_{ij} = -a_{ij} (i \neq j)$ and $l_{ii} = \sum_{m=1,m\neq i}^{N} a_{im}$. We define $\mathcal{P}_{\mathrm{N}} = diag\{b_1, \cdots, b_N\}$, $b_i = 0$ denotes the i-th following vehicle cannot obtain communication

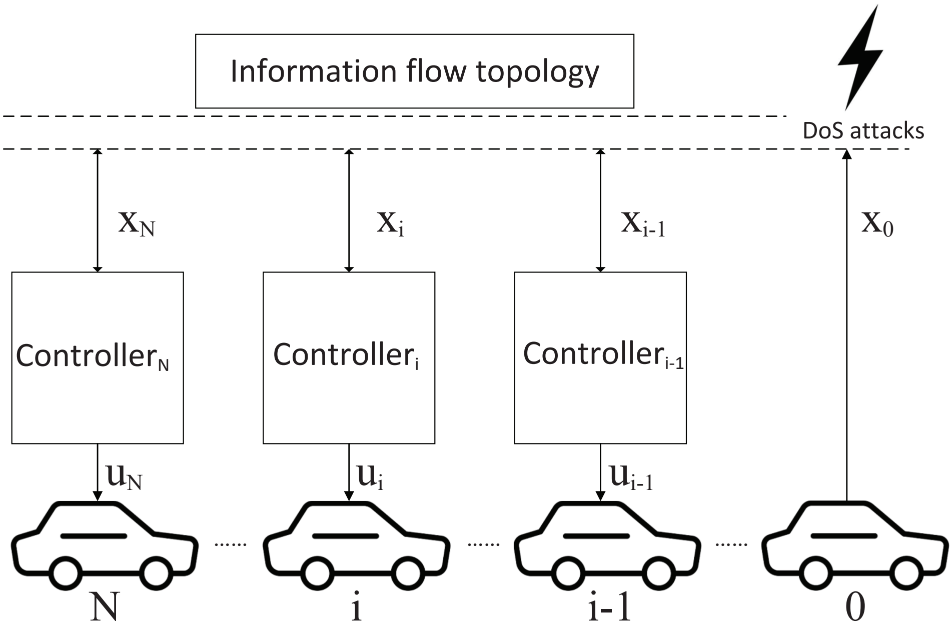


Figure 1. System structure.

from the leading vehicle; otherwise, $b_i = 1$.

2.2. Vehicle model

The longitudinal dynamics model of a vehicle is nonlinear in practice. The vehicle model has been linearized in many articles by using feedback linearization techniques to simplify the analysis[33,34]. In this paper, it is assumed that the longitudinal dynamics of the i-th following vehicle and the leading vehicle are given as follows[35,36]:

$$\dot{x}_i(t) = \bar{A}_i x_i(t) + \bar{B}_i u_i(t) \tag{1}$$

$$\dot{x}_0(t) = \bar{A}_0 x_0(t) \tag{2}$$

where

$$x_i(t) = \begin{bmatrix} p_i(t) \\ v_i(t) \\ a_i(t) \end{bmatrix}, x_0(t) = \begin{bmatrix} p_0(t) \\ v_0(t) \\ a_0(t) \end{bmatrix}, \bar{A}_i = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -\frac{1}{\sigma_i} \end{bmatrix}, \bar{B}_i = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{\sigma_i} \end{bmatrix}, \bar{A}_0 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -\frac{1}{\sigma_0} \end{bmatrix}$$

with $p_i(t)$, $v_i(t)$, $a_i(t)$, and $u_i(t)$ being the position, velocity, acceleration, and control input of the i-th following vehicle, respectively. $p_0(t)$, $v_0(t)$, and $a_0(t)$ are the position, velocity, and acceleration of the leading vehicle, respectively. σ_i and σ_0 denote the engine inertia time constant for the i-th following vehicle and the leading vehicle. In this paper, we consider the case that all vehicles have the same mathematical models.

By discretizing systems Equations (1) and (2), we can obtain the following discrete-time systems[33]

$$x_i(k+1) = Ax_i(k) + Bu_i(k) \tag{3}$$

$$x_0(k+1) = Ax_0(k) \tag{4}$$

$$A = \begin{bmatrix} 1 & T & 0.5T^2 \\ 0 & 1 & T \\ 0 & 0 & 1 - \frac{1}{\sigma}T \end{bmatrix}, B = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{\sigma}T \end{bmatrix}$$

where T is the sampling period, and $\sigma > 0$ is the vehicle engine inertia time constant.

2.3. DoS attacks

In this paper, it is assumed that all communication channels are blocked, and all following vehicles cannot receive any real-time data when DoS attacks occur. Define $\{k_j\}_{j\in\mathcal{N}^+}$ be the moment when DoS attacks occur, and τ_j is the duration of the j-th DoS attacks, where $\tau_j \geq 0$. Define the activated time interval at j-th DoS attacks as[37]

$$\mathrm{H}_j = \{k_j\} \cup [k_j, k_j + \tau_j)$$

Define $\Psi(\omega, k)$ and $\Gamma(\omega, k)$ as the time interval sets that the DoS attacks are active and inactive in the time interval $[\omega, k]$, respectively. $\Psi_{tot}(\omega, k)$ and $\Gamma_{tot}(\omega, k)$ represent the lengths of $\Psi(\omega, k)$ and $\Gamma(\omega, k)$, respectively. Define ϕ as the DADR in the time interval $[\omega, k]$, where $\phi = \frac{\Psi_{tot}}{k-\omega}$. The descriptions corresponding to this statement are as follows:

$$\Psi(\omega, k) = \bigcup_{j\in\mathcal{N}^+} H_j \bigcap [\omega, k], \Gamma(\omega, k) = [\omega, k] \setminus \Psi(\omega, k).$$

Then, two assumptions about the frequency and duration of DoS attacks are given. $n(\omega, k)$ is the number of DoS attacks occurring in the time interval $[\omega, k]$.

Assumption 1 (DoS attacks frequency): There exist positive constants $\kappa \in R_{\geq 0}$ and $\tau_D \in R_{>0}$, satisfying

$$n(\omega, k) \leq \kappa + \frac{k-\omega}{\tau_D}$$

for all $\omega, k \in R_{\geq 0}$ with $k > \omega$.

Assumption 2: For the duration of DoS attacks, there exist positive constants $\eta \in R_{\geq 0}$ and $T_a \in R_{>1}$, satisfying

$$\Psi_{tot}(\omega, k) \leq \eta + \frac{k-\omega}{T_a}$$

for all $\omega, k \in R_{\geq 0}$ with $k > \omega$. We assume that $\eta + \frac{k-\omega}{T_a}$ is the maximum total duration of DoS attacks in the time interval $[\omega, k]$.

Remark 1: The behavior of DoS attacks has been studied in many articles[37–39]. However, in practical applications, it is difficult to determine the accurate statistical parameters of DoS attacks for controller design. Considering that the energy of attackers is limited, we model DoS attacks by the frequency and duration parameters under Assumption 1 and Assumption 2. Such a modeling approach can also be found in Ref.[37,40], which can capture a wide range of different types of DoS attacks. Therefore, Assumption 1 and Assumption 2 are physically meaningful.

Remark 2: There are two methods to control the system when DoS attacks occur. One sets the system control input to zero, and the other keeps the system input of the last value. When DoS attacks occur, the hold input method can be used to update the control input with past data in the buffer, but it can also cause the time delay phenomenon. It is worth noting that both of the above methods are applicable[41]. In our work, the zero-input method is used.

2.4. Problem description

To control the CVP system, the following control protocol is introduced[21]:

$$\begin{aligned} u_i(k) = \sum_{j=1,j\neq i}^{N} & a_{ij}[k_p(p_i(k) - p_j(k) - d_{ij}) + k_v(v_i(k) - v_j(k)) + k_a(a_i(k) - a_j(k))] \\ & + b_i[k_p(p_i(k) - p_0(k) - d_{i0}) + k_v(v_i(k) - v_0(k)) + k_a(a_i(k) - a_0(k))] \end{aligned} \tag{5}$$

where k_p, k_v, and k_a are the local feedback gains of the system. d_{ij} is the ideal distance between the i-th and the j-th following vehicle. d_{i0} is the ideal distance between the i-th following vehicle and the leading vehicle.

Define the tracking error as

$$\begin{cases} \bar{p}_i(k) = p_i(k) - p_0(k) - d_{i0} \\ \bar{v}_i(k) = v_i(k) - v_0(k) \\ \bar{a}_i(k) = a_i(k) - a_0(k) \end{cases}$$

where $\bar{p}_i(k)$, $\bar{v}_i(k)$, and $\bar{a}_i(k)$ represent the position error, velocity error, and acceleration error of the actual and ideal state of the i-th following vehicle at the sampling time k, respectively. Let $K = [k_p, k_v, k_a]$ represent the controller gain.

Then the protocol Equation (5) can be written as

$$u_i(k) = \sum_{j=1, j\neq i}^{N} a_{ij}[K(e_i(k) - e_j(k))] + b_i K e_i(k) \tag{6}$$

where $e_i(k) = \begin{bmatrix} \bar{p}_i^T(k) & \bar{v}_i^T(k) & \bar{a}_i^T(k) \end{bmatrix}^T$.

The main goal of this paper is to maintain the ideal spacing, speed, and acceleration between the following vehicle and the leading vehicle. So, the desired state equation of the i-following vehicle is

$$x_0(k+1) + \Delta x = A x_0(k) + \Delta x \tag{7}$$

where $\Delta x = \begin{bmatrix} d_{i0} & 0 & 0 \end{bmatrix}$.

The actual state equation of the i-th following vehicle is

$$x_i(k+1) = A x_i(k) + BK \left\{ \left[\sum_{j=1, j\neq i}^{N} a_{ij}(e_i(k) - e_j(k)) \right] + b_i e_i(k) \right\} \tag{8}$$

Through Equation (7) and Equation (8), the tracking error of the i-th following vehicle is obtained as follows:

$$\begin{aligned} e_i(k+1) &= x_i(k+1) - x_0(k+1) \\ &= A e_i(k) + BK \left\{ \left[\sum_{j=1, j\neq i}^{N} a_{ij}(e_i(k) - e_j(k)) \right] + b_i e_i(k) \right\} \end{aligned} \tag{9}$$

Let $e(k) = \begin{bmatrix} e_1{}^T(k) & e_2{}^T(k) & \cdots & e_N{}^T(k) \end{bmatrix}^T$ and $u(k) = \begin{bmatrix} u_1{}^T(k) & u_2{}^T(k) & \cdots & u_N{}^T(k) \end{bmatrix}^T$, we can get

$$e(k+1) = [I_N \otimes A + (\mathcal{L}_N + \mathcal{P}_N) \otimes BK] e(k) \tag{10}$$

Due to the fact that no data can be received by those vehicles when the DoS attack occurs, we now introduce a signal $\delta(k) \in \{0, 1\}$ to describe whether the DoS attacks occur or not. Then the system can be described as

$$\begin{cases} \delta(k) = 0 : e(k+1) = [I_N \otimes A + (\mathcal{L}_N + \mathcal{P}_N) \otimes BK] e(k) \\ \delta(k) = 1 : e(k+1) = (I_N \otimes A) e(k) \end{cases} \tag{11}$$

Let $\mathcal{H}_N = \mathcal{L}_N + \mathcal{P}_N$. It follows from Equation (11) that the system under DoS attacks is essentially a switched system with two subsystems. Thus, Equation (11) can be written as

$$e(k+1) = [I_N \otimes A + \delta(k) \mathcal{H}_{\mathrm{N}} \otimes BK] e(k) \tag{12}$$

Define T_j and $\mathrm{T}_j{}^-$ as the j-th switching instant of $\delta(k)$ and the instant immediately before reaching T_j. The following lemma and definition will be used in the derivation of the main results.

Lemma 1[42]: Since the matrix $\mathcal{H}_N$ is a symmetric non-singular matrix, there exists an orthogonal matrix M, satisfying

$$M \mathcal{H}_{\mathrm{N}} M^T = diag(\lambda_1, \lambda_2, ..., \lambda_N) = \Lambda \tag{13}$$

where $\lambda_i (i = 1, 2, ..., N)$ are the eigenvalues of $\mathcal{H}_{\mathrm{N}}$.

Definition 1[43]: If there exist constant $\rho \in (0, +\infty)$ and $\varsigma \in (0, 1)$ such that

$$|e(k)| \leq \rho \varsigma^k ||e(0)||, \quad k = 1, 2, ... \tag{14}$$

is true, then the system Equation (12) is said to be exponentially stable, and ς is the exponential decay rate.

3. MAIN RESULTS

In this section, we will analyze the exponential stability of the system Equation (12) with the designed controller Equation (5), and then the main results of the controller design based on the DMPC will be given. Before this, we construct the Lyapunov function for Equation (12) as

$$V(k) = \begin{cases} V_0(k), \delta(k) = 0 \\ V_1(k), \delta(k) = 1 \end{cases} \tag{15}$$

where $V_0(k) = e^T(k)(I_N \otimes P_0)e(k)$ and $V_1(k) = e^T(k)(I_N \otimes P_1)e(k)$.

3.1. Stability analysis

The main theorems in this section are given as follows to demonstrate that system Equation (12) can be exponentially stable with the designed controller Equation (5). Define the total number of switches in the time interval $[0, k]$ as $n = n(0, k) + n_1$. If the system switches to the case of no DoS attacks in the end, then $n_1 = n(0, k)$; otherwise, $n_1 = n(0, k) - 1$.

Theorem 1: Considering the parameters of DoS attacks as in Assumption 1 and Assumption 2. For the given positive scalars $\alpha \in (0, 1)$, $\beta \in (0, +\infty)$, and $\mu \in (1, +\infty)$, if there exists a positive constant $\theta \in (1, +\infty)$ and symmetric positive definite matrices, P_0 and P_1, such that

$$\frac{\ln \mu}{\tau_D} \leq \ln \theta \tag{16}$$

$$\frac{\ln(1+\beta) + \ln(\frac{1}{1-\alpha})}{T_a} \leq \ln(\frac{1}{1-\alpha}) - \varphi \ln \theta \tag{17}$$

$$(A + \lambda_{\max} BK)^T P_0 (A + \lambda_{\max} BK) - (1-\alpha) P_0 \leq 0 \tag{18}$$

$$A^T P_1 A - (1+\beta) P_1 \leq 0 \tag{19}$$

$$P_0 \leq \mu P_1 \tag{20}$$

$$P_1 \leq \mu P_0 \tag{21}$$

hold, then the system (12) can be ensured to be exponentially stable with an exponential decay rate of $\theta^{-\frac{(\varphi-2)}{2}}$, $\varphi > 2$, where λ_{max} is the maximum eigenvalue of $\mathcal{H}_{\mathrm{N}}$.

Proof: When $k \in \Gamma(\omega, k)$, by left- and right-multiplying Equation (18) by ${e_i}^T(k)$ and its transposition, respectively, one can see that

$${e_i}^T(k)[(A + \lambda_{\max} BK)^T P_0 (A + \lambda_{\max} BK) - (1-\alpha) P_0] e_i(k) \leq 0 \tag{22}$$

Then we have

$$e^T(k)[(I_N \otimes A + \Lambda \otimes BK)^T (I_N \otimes P_0)(I_N \otimes A + \Lambda \otimes BK) - (1-\alpha)(I_N \otimes P_0)] e(k) \leq 0 \tag{23}$$

Let $\varepsilon(k) = (M^T \otimes I_N)e(k)$, with the help of Lemma 1, Equation (23) can be written as

$$\varepsilon^T(k)[(I_N \otimes A + \mathcal{H}_{\mathrm{N}} \otimes BK)^T(I_N \otimes P_0)(I_N \otimes A + \mathcal{H}_{\mathrm{N}} \otimes BK) - (1-\alpha)(I_N \otimes P_0)]\varepsilon(k) \leq 0 \tag{24}$$

Thus, it is obtained that

$$(I_N \otimes A + \mathcal{H}_{\mathrm{N}} \otimes BK)^T(I_N \otimes P_0)(I_N \otimes A + \mathcal{H}_{\mathrm{N}} \otimes BK) - (1-\alpha)(I_N \otimes P_0) \leq 0 \tag{25}$$

Now left- and right-multiplying Equation (25) by $e^T(k)$ and its transposition, respectively, yields

$$e^T(k)[(I_N \otimes A + \mathcal{H}_{\mathrm{N}} \otimes BK)^T(I_N \otimes P_0)(I_N \otimes A + \mathcal{H}_{\mathrm{N}} \otimes BK) - (1-\alpha)(I_N \otimes P_0)]e(k) \leq 0 \tag{26}$$

Considering the Lyapunov function Equation (15), Equation (26) can be written as

$$V_0(k+1) - V_0(k) \leq -\alpha V_0(k), k \in \Gamma(\omega, k) \tag{27}$$

When $k \in \Psi(\omega, k)$, by left- and right-multiplying Equation (19) by ${e_i}^T(k)$ and its transposition, respectively, one can see that

$${e_i}^T(k)[A^T P_1 A - (1+\beta)P_1]e_i(k) \leq 0 \tag{28}$$

Obviously, Equation (28) can guarantee that

$$e^T(k)[(I_N \otimes A)^T(I_N \otimes P_1)(I_N \otimes A) - (1+\beta)(I_N \otimes P_1)]e(k) \leq 0 \tag{29}$$

Similar to the derivation of Equation (27), Equation (29) can be written as

$$V_1(k+1) - V_1(k) \leq \beta V_0(k), k \in \Psi(\omega, k) \tag{30}$$

Thus, the conditions Equation (18) and Equation (19) can guarantee that

$$\begin{cases} V_0(k+1) \leq (1-\alpha)V_0(k), & \delta(k) = 0 \\ V_1(k+1) \leq (1+\beta)V_1(k), & \delta(k) = 1 \end{cases} \tag{31}$$

Considering the conditions Equation (20) and Equation (21), one has

$$\begin{cases} V_0(\mathrm{T}_j) \leq \mu V_1({\mathrm{T}_j}^-), & \delta({\mathrm{T}_j}^-) = 1 \ and \ \delta(\mathrm{T}_j) = 0 \\ V_1(\mathrm{T}_j) \leq \mu V_0({\mathrm{T}_j}^-), & \delta({\mathrm{T}_j}^-) = 0 \ and \ \delta(\mathrm{T}_j) = 1 \end{cases} \tag{32}$$

According to Equation (31) and Equation (32) and by applying the iterative method to the time interval $[0, k]$, we can obtain

$$\begin{aligned} V_{\delta(k)}(k) &\leq \mu^{n(0,k)+n_1}(1+\beta)^{\Psi_{tot}(0,k)}(1-\alpha)^{\Gamma_{tot}(0,k)}V_{\delta(0)}(0) \\ &\leq \mu^{2n(0,k)}(1+\beta)^{\eta+\frac{k-0}{Ta}}(\frac{1}{1-\alpha})^{\eta+\frac{k-0}{Ta}-k}V_{\delta(0)}(0) \\ &\leq \mu^{2(\kappa+\frac{k-0}{\tau_D})}(1+\beta)^{\eta+\frac{k}{Ta}}(\frac{1}{1-\alpha})^{\eta+\frac{k}{Ta}-k}V_{\delta(0)}(0) \\ &= \mu^{2\kappa}(\frac{1+\beta}{1-\alpha})^{\eta}\mu^{\frac{2k}{\tau_D}}(1+\beta)^{\frac{k}{Ta}}(\frac{1}{1-\alpha})^{(\frac{1}{Ta}-1)k}V_{\delta(0)}(0) \\ &= \mu^{2\kappa}(\frac{1+\beta}{1-\alpha})^{\eta}e^{\frac{2k}{\tau_D}\ln\mu}e^{\frac{k}{Ta}\ln(1+\beta)}e^{(\frac{1}{Ta}-1)k\ln(\frac{1}{1-\alpha})}V_{\delta(0)}(0) \end{aligned} \tag{33}$$

The conditions Equation (16) and Equation (17) guarantee that

$$\begin{aligned} V_{\delta(k)}(k) &\leq \mu^{2\kappa}(\frac{1+\beta}{1-\alpha})^{\eta}e^{2k\ln\theta}e^{-\varphi k\ln\theta}V_{\delta(0)}(0) \\ &= \mu^{2\kappa}(\frac{1+\beta}{1-\alpha})^{\eta}e^{(2-\varphi)k\ln\theta}V_{\delta(0)}(0) \\ &= \mu^{2\kappa}(\frac{1+\beta}{1-\alpha})^{\eta}\theta^{-(\varphi-2)k}V_{\delta(0)}(0) \end{aligned} \tag{34}$$

Let $c = \mu^{2\kappa}(\frac{1+\beta}{1-\alpha})^{\eta} \in R_{>0}$, Equation (34) can be written as

$$a|e(k)|^2 \le V_{\delta(k)}(k) \le c\theta^{-(\varphi-2)k} b\|e(0)\|^2 \tag{35}$$

where $a = \lambda_{\min}(P_{\delta(k)})$ and $b = \lambda_{\max}(P_{\delta(0)})$. $\lambda_{\min}(P_{\delta(k)})$ is the minimum eigenvalue of $P_{\delta(k)}$ and $\lambda_{\max}(P_{\delta(0)})$ is the maximum eigenvalue of $P_{\delta(0)}$.
Then it yields

$$|e(k)| \le \sqrt{\frac{bc}{a}}\theta^{-\frac{(\varphi-2)k}{2}}\|e(0)\| \tag{36}$$

From Equation (36) and Definition 1, the system (12) is exponentially stable with an exponential decay rate of $\theta^{-\frac{(\varphi-2)}{2}}$. This ends the proof.

It follows from Theorem 1 that for given α, β, μ and DoS attacks parameters κ, τ_D, η, T_a, we have

$$|e(k)| \le \sqrt{\frac{bc}{a}}\left[(1-\alpha)^{\frac{1}{2}}\mu^{\frac{1}{2\tau_D}}\left(\frac{1+\beta}{1-\alpha}\right)^{\frac{1}{2T_a}}\right]^k\|e(0)\| \tag{37}$$

With the help of Definition 1, the exponential decay rate ς can be written as

$$\varsigma = (1-\alpha)^{\frac{1}{2}}\mu^{\frac{1}{2\tau_D}}\left(\frac{1+\beta}{1-\alpha}\right)^{\frac{1}{2T_a}} \tag{38}$$

Remark 3: In the previous section, a quantitative relationship between DoS attack parameters and the exponential decay rate has been established. It can be seen that both the frequency and duration of DoS attacks have an impact on the exponential decay rate, which affects the performance of the system. For example, as the duration of DoS attacks increases, the exponential decay rate becomes larger.

3.2. Upper bound of DADR

As it is well known, if the total duration of a DoS attack is infinite, the system cannot be stable. Therefore, it is necessary to derive the upper bound of DARA for the system (12). To achieve this, we present the stability theorem as follows based on the DARA:

Theorem 2: For the given positive scalars $\alpha \in (0,1)$, $\beta \in (0,+\infty)$, and $\mu \in (1,+\infty)$, if the upper bound of DARA is $\phi < \phi_{\max} = \frac{-\frac{2\ln\mu}{\tau_D}-\ln(1-\alpha)}{\ln\left(\frac{1+\beta}{1-\alpha}\right)}$, and if there exists a positive scalar $\theta \in (1,+\infty)$ and symmetric positive definite matrices, P_0 and P_1, such that the inequalities Equation (18)-Equation (21) hold, then the system (12) is exponentially stable.

Proof: Similarly to the analysis in Theorem 1, we can obtain

$$\begin{aligned}
V_{\delta(k)}(k) &\le \mu^{n(0,k)+n_1}(1+\beta)^{\Psi_{tot}(0,k)}(1-\alpha)^{\Gamma_{tot}(0,k)}V_{\delta(0)}(0)\\
&\le \mu^{2n(0,k)}(1+\beta)^{\Psi_{tot}(0,k)}(1-\alpha)^{k-\Psi_{tot}(0,k)}V_{\delta(0)}(0)\\
&\le \mu^{2(\kappa+\frac{k-0}{\tau_D})}(1+\beta)^{\phi k}(1-\alpha)^{k-\phi k}V_{\delta(0)}(0)\\
&= \mu^{2\kappa}e^{\frac{2k}{\tau_D}\ln\mu}e^{\phi k\ln(1+\beta)}e^{(k-\phi k)\ln(1-\alpha)}V_{\delta(0)}(0)\\
&= \mu^{2\kappa}e^{\left(\frac{2}{\tau_D}\ln\mu+\phi\ln(\frac{1+\beta}{1-\alpha})+\ln(1-\alpha)\right)k}V_{\delta(0)}(0)
\end{aligned} \tag{39}$$

Similarly to Equation (35), we can obtain

$$|e(k)| \le \sqrt{\frac{b}{a}}\mu^{\kappa}\left(e^{\frac{1}{2}\left[\frac{2}{\tau_D}\ln\mu+\phi\ln(\frac{1+\beta}{1-\alpha})+\ln(1-\alpha)\right]}\right)^k\|e(0)\| \tag{40}$$

By substituting $\phi < \phi_{\max} = \frac{-\frac{2\ln\mu}{\tau_D} - \ln(1-\alpha)}{\ln\left(\frac{1+\beta}{1-\alpha}\right)}$ to Equation (40), we can obtain that $\frac{2}{\tau_D}\ln\mu + \phi\ln(\frac{1+\beta}{1-\alpha}) + \ln(1-\alpha) < 0$ and $0 < e^{\frac{1}{2}\left[\frac{2}{\tau_D}\ln\mu + \phi\ln(\frac{1+\beta}{1-\alpha}) + \ln(1-\alpha)\right]} < 1$. From Definition 1, the system (12) is exponentially stable. This completes the proof.

3.3. Controller design

Based on Theorem 1, we now present the robust model predictive control algorithm. The state feedback control gain will be obtained by solving an optimization problem in the form of linear matrix inequalities (LMIs) at each sampling moment. The following theorem gives the design of the controller.

Theorem 3: Considering a CVP system consists of the plant Equation (12) and the controller Equation (5). Let $e(k) = e(k|k)$ be the state of the system (12) measured at sampling time k. DoS attack parameters satisfy conditions Equation (16) and Equation (17). For the given constant scalar $u_{\max}$ and positive scalars $0 < \alpha < 1$, $\beta > 0$, $\mu > 1$, $\theta > 1$, and $\varphi > 2$, if there exist matrices, Q_0, Q_1, and Y, and a positive scalar $\gamma > 0$ such that

$$\min \gamma \tag{41}$$

subject to

$$\begin{bmatrix} -1 & * \\ e(k) & I_N \otimes (-Q_0) \end{bmatrix} \leq 0 \tag{42}$$

$$\begin{bmatrix} -(1-\alpha)Q_0 & * & * & * \\ AQ_0 + \lambda_{\max} BY & -Q_0 & * & * \\ W^{\frac{1}{2}} Q_0 & 0 & -\gamma I & * \\ \lambda_{\max} R^{\frac{1}{2}} Y & 0 & 0 & -\gamma I \end{bmatrix} \leq 0 \tag{43}$$

$$\begin{bmatrix} -(u_{\max})^2 & * \\ Y^T & -\frac{1}{m} Q_0 \end{bmatrix} \leq 0 \tag{44}$$

$$\begin{bmatrix} -(1-\alpha)Q_0 & * \\ AQ_0 + \lambda_{\max} BY & -Q_0 \end{bmatrix} \leq 0 \tag{45}$$

$$\begin{bmatrix} -(1+\beta)Q_1 & * \\ AQ_1 & -Q_1 \end{bmatrix} \leq 0 \tag{46}$$

$$\begin{bmatrix} -\mu Q_0 & * \\ Q_0 & -Q_1 \end{bmatrix} \leq 0 \tag{47}$$

$$\begin{bmatrix} -\mu Q_1 & * \\ Q_1 & -Q_0 \end{bmatrix} \leq 0 \tag{48}$$

where $Q_0 = \gamma {P_0}^{-1}$, $Q_1 = \gamma {P_1}^{-1}$, and $Y = KQ_0$. If there is a solution to the above linear minimization problem, then the state feedback matrix K with sampling moment k can be obtained by the following equation:

$$K = Y{Q_0}^{-1} \tag{49}$$

and the system (12) can be ensured to be exponentially stable with an exponential decay rate of $\theta^{-\frac{(\varphi-2)}{2}}$.

Proof: We aim to design a state feedback control law at each sampling time that minimizes an infinite horizon global objective function. First, we define the infinite horizon local objective function for the i-th following vehicle in the CVP as

$$J_{i,\infty}(k) = \sum_{t=0}^{\infty} \left[{e_i}^T(k+t|k)\, We_i(k+t|k) + {u_i}^T(k+t|k)\, Ru_i(k+t|k) \right] \tag{50}$$

where $e_i\left(k+t|k\right)$ and $u_i\left(k+t|k\right)$ represent the predictions of state and control input at sampling time k, and W and R are state and control weighting matrices, respectively.
Adding up the infinite horizon local objective function of all following vehicles as the global objective function, so the global objective function is

$$\begin{aligned} J_\infty(k) &= \sum_{i=1}^{N}\sum_{t=0}^{\infty}\left[{e_i}^T\left(k+t|k\right)We_i\left(k+t|k\right)+{u_i}^T\left(k+t|k\right)Ru_i\left(k+t|k\right)\right] \\ &= \sum_{t=0}^{\infty}\left[e^T\left(k+t|k\right)\left(I_N\otimes W\right)e\left(k+t|k\right)+u^T\left(k+t|k\right)\left(I_N\otimes R\right)u\left(k+t|k\right)\right] \end{aligned} \tag{51}$$

Left- and right-multiplying Equation (43) by $diag\{{Q_0}^{-1}, I, I, I\}$ and its transposition, respectively. By Schur complement, one has

$$-(1-\alpha)P_0+(A+\lambda_{\max}BK)^TP_0(A+\lambda_{\max}BK)+W+{\lambda_{\max}}^2K^TRK\leq 0 \tag{52}$$

Left- and right-multiplying Equation (52) by ${e_i}^T(k)$ and its transposition, respectively, yields

$${e_i}^T(k)[-(1-\alpha)P_0+(A+\lambda_{\max}BK)^TP_0(A+\lambda_{\max}BK)+W+{\lambda_{\max}}^2K^TRK]e_i(k)\leq 0 \tag{53}$$

Then, it can be derived

$$e^T(k)[-I_N\otimes(1-\alpha)P_0+{\Pi_1}^T(I_N\otimes P_0)\Pi_1+I_N\otimes W+(\Lambda\otimes K)^T(I_N\otimes R)(\Lambda\otimes K)]e(k)\leq 0 \tag{54}$$

where $\Pi_1=I_N\otimes A+\Lambda\otimes BK$. Let $\varepsilon(k)=(M^T\otimes I_N)e(k)$, and with the help of Lemma 1, Equation (54) can be written as

$$\varepsilon^T(k)[-I_N\otimes(1-\alpha)P_0+{\Pi_2}^T(I_N\otimes P_0)\Pi_2+I_N\otimes W+(\mathcal{H}_{\mathrm{N}}\otimes K)^T(I_N\otimes R)(\mathcal{H}_{\mathrm{N}}\otimes K)]\varepsilon(k)\leq 0 \tag{55}$$

where $\Pi_2=I_N\otimes A+\mathcal{H}_{\mathrm{N}}\otimes BK$. Obviously, Equation (55) guarantees that

$$-I_N\otimes(1-\alpha)P_0+{\Pi_2}^T(I_N\otimes P_0)\Pi_2+I_N\otimes W+(\mathcal{H}_{\mathrm{N}}\otimes K)^T(I_N\otimes R)(\mathcal{H}_{\mathrm{N}}\otimes K)\leq 0 \tag{56}$$

Left- and right-multiplying Equation (56) by $e^T(k+t|k)$ and its transposition, respectively, yields

$$e^T(k+t|k)[-I_N\otimes(1-\alpha)P_0+{\Pi_2}^T(I_N\otimes P_0)\Pi_2+I_N\otimes W+(\mathcal{H}_{\mathrm{N}}\otimes K)^T(I_N\otimes R)(\mathcal{H}_{\mathrm{N}}\otimes K)]e(k+t|k)\leq 0 \tag{57}$$

which leads to

$$V_0\left(k+t+1|k\right)-(1-\alpha)V_0\left(k+t|k\right)\leq-(\Pi_3+\Pi_4) \tag{58}$$

where $\Pi_3=e^T(k+t|k)\left(I_N\otimes W\right)e(k+t|k)$ and $\Pi_4=u^T(k+t|k)\left(I_N\otimes R\right)u(k+t|k)$. Therefore, the condition Equation (43) can guarantee that Equation (58) hold. Then it can be obtained from Equation (58) that

$$(\Pi_3+\Pi_4)\leq(1-\alpha)V_0\left(k+t|k\right)-V_0\left(k+t+1|k\right)\leq V_0\left(k+t|k\right)-V_0\left(k+t+1|k\right) \tag{59}$$

Let Equation (59) be an iterative summation from $t=0$ to $t=\infty$, one has

$$V_0\left(k+\infty|k\right)-V_0\left(k+0|k\right)\leq-\sum_{t=0}^{\infty}\left[e^T(k+t|k)\left(I_N\otimes W\right)e(k+t|k)+u^T(k+t|k)\left(I_N\otimes R\right)u(k+t|k)\right] \tag{60}$$

In order to make the robust performance objective function finite, we define $e(k+\infty|k)=0$, so Equation (60) can be written as

$$J_\infty(k)\leq V_0\left(k+0|k\right)=V_0\left(k\right)=e^T(k)(I_N\otimes P_0)e(k)\leq\gamma \tag{61}$$

By Schur complement, Equation (61) can be rewritten as

$$\begin{bmatrix} 1 & e^T(k) \\ e(k) & I_N\otimes\gamma{P_0}^{-1} \end{bmatrix}\leq 0 \tag{62}$$

By substituting $Q_0 = \gamma P_0{}^{-1}$ to Equation (62), it can be seen that Equation (42) and Equation (61) are equivalent.

The control input of any following vehicles in CVP control is constrained. For the i-th following vehicle, satisfying $\|u_i(k)\|^2 \leq (u_{\max})^2$

$$\begin{aligned} \|u_i(k)\|^2 &\leq \left\| \sum_{j=1, j\neq i}^{N} a_{ij}[K(e_i(k) - e_j(k))] + b_i K e_i(k) \right\|_2^2 \\ &= \left\| \sum_{j=1, j\neq i}^{N} a_{ij}[YQ^{-1}(e_i(k) - e_j(k))] + b_i YQ^{-1} e_i(k) \right\|_2^2 \\ &\leq m \left\| YQ^{-\frac{1}{2}} \right\|_2^2 \leq (u_{\max})^2 \end{aligned} \tag{63}$$

where $m = \max\left\{ b_1 + 2 * \sum_{j=1}^{N} a_{1j}, b_2 + 2 * \sum_{j=1}^{N} a_{2j}, \cdots, b_N + 2 * \sum_{j=1}^{N} a_{Nj} \right\}$.
By using Schur complement, the condition Equation (44) can guarantee that Equation (63) holds.

Left- and right-multiplying Equation (45) by $diag\{Q_0{}^{-1}, I\}$ and its transposition, respectively, it is obtained that

$$-(1-\alpha)Q_0{}^{-1} + (A + \lambda_{\max} BK)^T Q_0{}^{-1}(A + \lambda_{\max} BK) \tag{64}$$

By substituting $Q_0 = \gamma P_0^{-1}$ into the previous equation, Equation (64) can be written as

$$-(1-\alpha)P_0 + (A + \lambda_{\max} BK)^T P_0 (A + \lambda_{\max} BK) \leq 0 \tag{65}$$

Left- and right-multiplying Equation (46) by $diag\{Q_1{}^{-1}, I\}$ and its transposition, respectively, yields

$$-(1+\beta)Q_1{}^{-1} + A^T Q_1{}^{-1} A \leq 0 \tag{66}$$

By substituting $Q_1 = \gamma P_1^{-1}$ into the previous equation, Equation (66) can be written as

$$-(1+\beta)Q_1{}^{-1} + A^T Q_1{}^{-1} A \leq 0 \tag{67}$$

Left- and right-multiplying Equation (47) by $diag\{Q_0{}^{-1}, I\}$ and its transposition, respectively, yields

$$-\mu Q_0{}^{-1} + Q_1{}^{-1} \leq 0 \tag{68}$$

By substituting $Q_1 = \gamma P_1^{-1}$ and $Q_0 = \gamma P_0^{-1}$ into the previous equation, Equation (68) can be written as

$$-\mu P_0 + P_1 \leq 0 \tag{69}$$

Left- and right-multiplying Equation (48) by $diag\{Q_1{}^{-1}, I\}$ and its transposition, respectively, yields

$$-\mu Q_1{}^{-1} + Q_0{}^{-1} \leq 0 \tag{70}$$

By substituting $Q_1 = \gamma P_1^{-1}$ and $Q_0 = \gamma P_0^{-1}$ into the previous equation, Equation (70) can be written as

$$-\mu P_1 + P_0 \leq 0 \tag{71}$$

With the help of Theorem 1, one can see that the hold of conditions Equation (45), Equation (46), Equation (47), Equation (48), Equation (16), and Equation (17) can guarantee that the system (12) is exponentially stable with an exponential decay rate of $\theta^{-\frac{(\varphi-2)}{2}}$. The controller gain can be obtained by solving an optimization problem based on the form of LMIs and $K = YQ_0{}^{-1}$. This completes the proof.

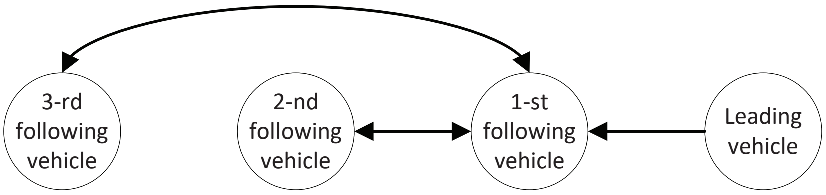
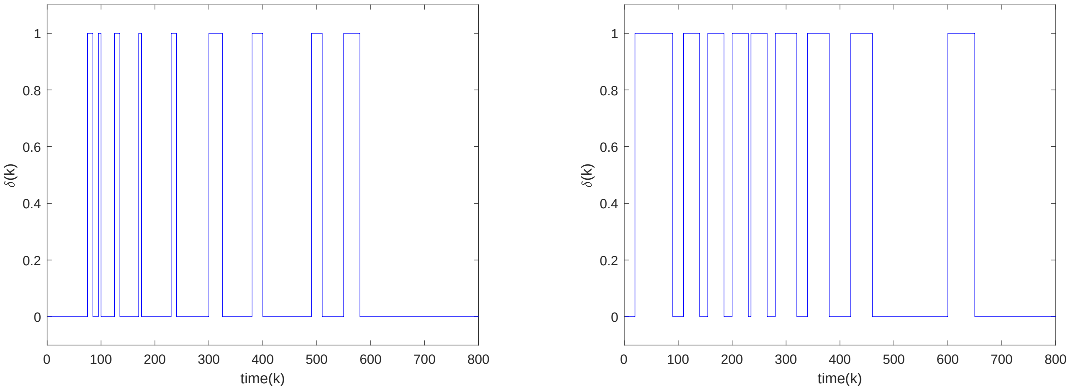


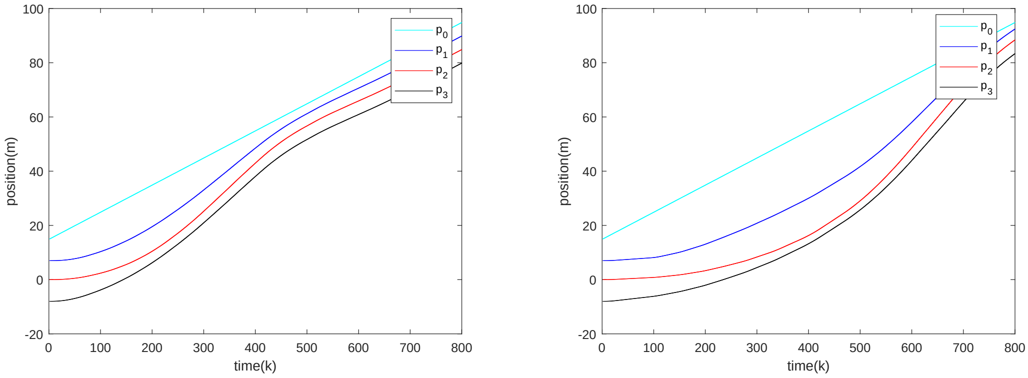
Figure 2. Communication topology.



(a) DoS attacks when ϕ = 16.875%.

(b) DoS attacks when ϕ = 45%.

Figure 3. DoS attacks.



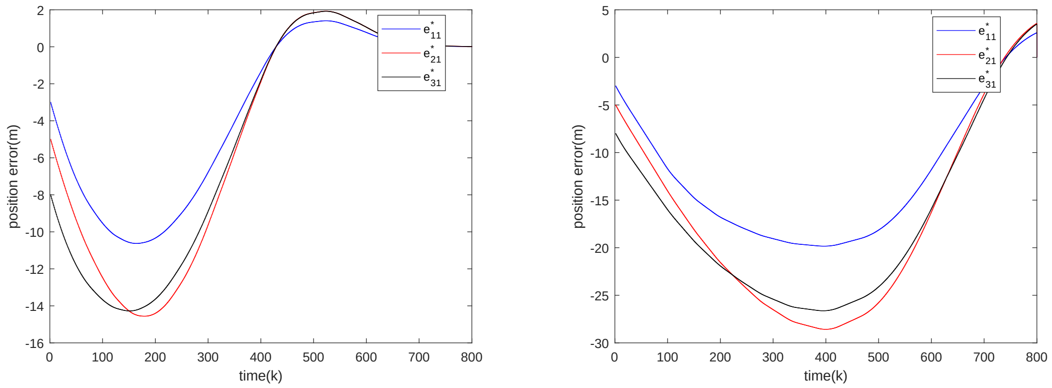
(a) Trajectories of position when ϕ = 16.875%.

(b) Trajectories of position when ϕ = 45%.

Figure 4. Trajectories of position.

4. SIMULATION

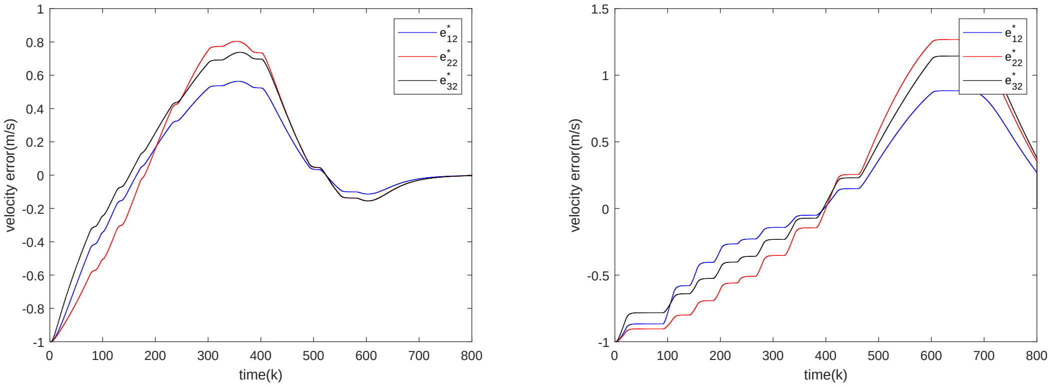
In this section, numerical simulations have been carried out using Matlab to illustrate the main results of this paper. Assuming that the CVP consists of one leading vehicle and three following vehicles and the communication topology is shown in Figure 2. We set the initial state of the leading vehicle to $x_0(0) = [\ 15 \quad 1 \quad 0\ ]^T$. The initial state of each of the three following vehicles is set to $x_1(0) = [\ 7 \quad 0 \quad 0\ ]^T$, $x_2(0) = [\ 0 \quad 0 \quad 0\ ]^T$ and $x_3(0) = [\ -8 \quad 0 \quad 0\ ]^T$. The maximum input $u_{\max} = 0.7$. The ideal vehicle spacing between vehicles to be $d_{i,i-1} = 5$m and $d_{i0} = 5 * i$m. We set vehicle engine inertia time constant $\sigma = 0.5$ and sampling period



(a) Trajectories of position error when ϕ = 16.875%.

(b) Trajectories of position error when ϕ = 45%.

Figure 5. Trajectories of position error.



(a) Trajectories of velocity error when ϕ = 16.875%.

(b) Trajectories of velocity error when ϕ = 45%.

Figure 6. Trajectories of velocity error.

$T = 0.1s$, so

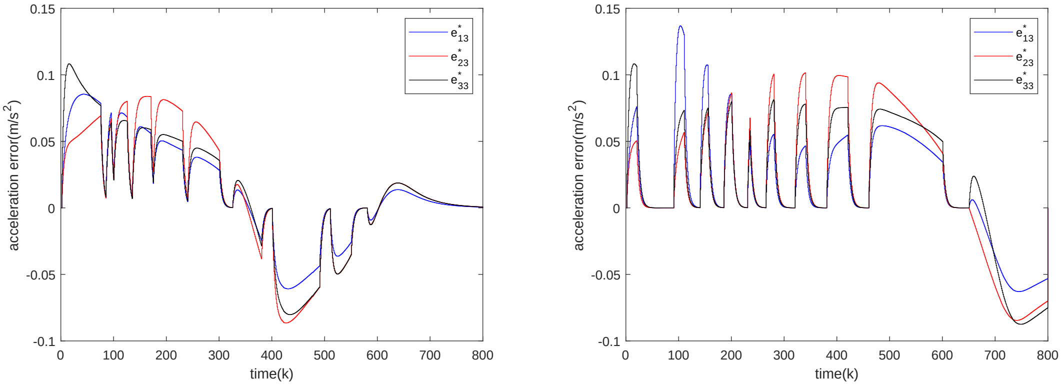
$$A = \begin{bmatrix} 1 & 0.1 & 0.005 \\ 0 & 1 & 0.1 \\ 0 & 0 & 0.8 \end{bmatrix}, B = \begin{bmatrix} 0 \\ 0 \\ 0.2 \end{bmatrix}.$$

The state and control weighting matrices $W = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, $R = 0.1$. Moreover, we choose the parameters in Theorem 3 as $\kappa = 0$, $\tau_D = 80$, $\eta = 0$, $\alpha = 0.022$, $\beta = 0.03$, $\mu = 1.04$, and $\varphi = 2.1$. The upper bound of DARA can be calculated as

$$\phi_{\max} = \frac{-\frac{2\ln\mu}{\tau_D} - \ln(1-\alpha)}{\ln\left(\frac{1+\beta}{1-\alpha}\right)} = \frac{-\frac{2\times\ln 1.04}{80} - \ln(1-0.022)}{\ln\left(\frac{1+0.03}{1-0.022}\right)} \approx 0.41.$$

So T_a can be calculated as $T_a = \frac{1}{\phi_{\max}} \approx 2.44$. By calculation, we can obtain

$$\ln\theta \geq \frac{\ln\mu}{\tau_D} = \frac{\ln 1.04}{80} \approx 0.00049$$



(a) Trajectories of acceleration error when $\phi = 16.875\%$.

(b) Trajectories of acceleration error when $\phi = 45\%$.

Figure 7. Trajectories of acceleration error.

$$\ln\theta \le \frac{\ln(\frac{1}{1-\alpha}) - \frac{\ln(1+\beta)+\ln(\frac{1}{1-\alpha})}{T_a}}{\varphi} = \frac{\ln(\frac{1}{1-0.022}) - \frac{\ln(1+0.03)+\ln(\frac{1}{1-0.022})}{2.44}}{2.1} \approx 0.0006$$

So there must exist a constant $\theta > 1$ such that our sufficient condition in Theorem 3 is satisfied. In the simulation, the DARAs are set to be $\phi = 16.875\%$ and $\phi = 45\%$, respectively.

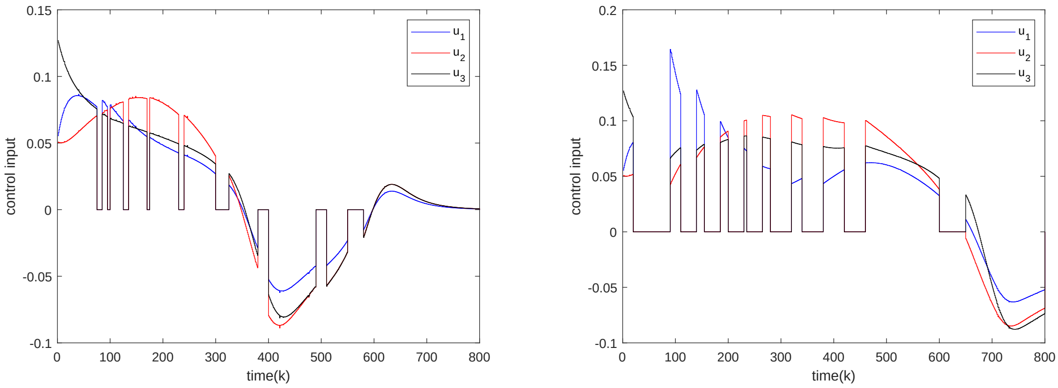
The sequence of DoS attacks is shown in Figure 3, where 0 indicates the normal case without DoS attacks and 1 indicates the occurrence of DoS attacks.

The position trajectories and position error trajectories are shown in Figure 4 and Figure 5, respectively, where ${e_{i1}}^* = p_i - p_0 - d_{i0}$. The velocity error trajectories are shown in Figure 6, where ${e_{i2}}^* = v_i - v_0$. The acceleration error trajectories are shown in Figure 7, where ${e_{i3}}^* = a_i - a_0$. When $\phi = 16.875\%$, Figure 5 shows that all vehicles can travel at the desired spacing. Figure 6 and Figure 7 show that all following vehicles can travel at the same speed and acceleration as the leading vehicle. When $\phi = 45\%$, it can be observed that the position errors, velocity errors, and acceleration errors of the following vehicles have not converged to zero in the time interval $[0, 800]$.

From the simulation results, it is evident that an increase in the DADR results in slower convergence of the system state error. Figure 8 shows the control input trajectories for the three following vehicles, and we can see that the control input satisfies the condition of $\|u_i(k)\|^2 \le (u_{\max})^2$.

5. CONCLUSION

A robust DMPC problem for a CVP system in the presence of DoS attacks has been investigated in this paper. A quantitative relationship has been established between the DoS attack parameters and the exponential decay rate. A distributed state feedback controller was designed by using the DMPC method to enable all following vehicles to track the velocity and acceleration of the leading vehicle exponentially and maintain the desired vehicle spacing. Finally, a CVP system consisting of one leading vehicle and three following vehicles was simulated on Matlab to demonstrate the effectiveness of our proposed control algorithm. However, the current work does not account for the presence of time delays and disturbances in the communication process. In future endeavors, attention will be focused on the distributed control of CVP systems with hybrid attacks and time delays.



(a) Control input when ϕ = 16.875%.

(b) Control input when ϕ = 45%.

Figure 8. Control input.

DECLARATIONS

Authors' contributions

Made substantial contributions to the research, idea generation, algorithm design, and simulation and wrote and edited the original draft: Zeng H

Performed critical review, commentary, and revision and provided administrative, technical, and material support: Ye Z, Zang D, and Lu Q

Availability of data and materials

Not applicable.

Financial support and sponsorship

None.

Conflicts of interest

All authors declared that there are no conflicts of interest.

Ethical approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Copyright

REFERENCES

1. Alam AA, Gattami A, Johansson KH. An experimental study on the fuel reduction potential of heavy duty vehicle platooning. In: 13th International IEEE Conference on Intelligent Transportation Systems; 2010. p. 306-11. DOI
2. Vegamoor VK, Darbha S, Rajagopal KR. A review of automatic vehicle following systems. *J Indian Inst Sci* 2019;99:567-87. DOI
3. Tsugawa S, Jeschke S, Shladover SE. A review of truck platooning projects for energy savings. *IEEE Trans Intell Veh* 2016;1:68-77. DOI
4. Hodge C, Hauck K, Gupta S, Bennett JC. Vehicle cybersecurity threats and mitigation approaches. tech. rep., National Renewable Energy Lab.(NREL), Golden, CO (United States), 2019. DOI
5. Parkinson S, Ward P, Wilson K, Miller J. Cyber threats facing autonomous and connected vehicles: future challenges. *IEEE Trans Intell Transport Syst* 2017;18:2898-915. DOI

6. 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;52:6246-58. DOI
7. 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;52:13486-99. DOI
8. Zhao N, Zhao X, Chen M, Zong G, Zhang H. Resilient distributed event-triggered platooning control of connected vehicles under denial-of-service attacks. *IEEE Trans Intell Transport Syst* 2023;24:6191-202. DOI
9. Merco R, Biron AB, Pisu P. Replay attack detection in a platoon of connected vehicles with cooperative adaptive cruise control. In: 2018 Annual American Control Conference (ACC); 2018. p. 5582-7 DOI
10. Ding D, Han Q, Xiang Y, Ge X, Zhang X. A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing* 2018;275:1674-83. DOI
11. Ju Z, Zhang H, Tan Y. Distributed deception attack detection in platoon-based connected vehicle systems. *IEEE Trans Veh Technol* 2020;69:4609-20. DOI
12. Naderi E, Asrari A. Integrated power and transportation systems targeted by false data injection cyberattacks in a smart distribution network. *Electric Transportation Systems in Smart Power Grids* Boca Raton: CRC Press; 2022. p. 447-72. DOI
13. Deng C, Zhang D, Feng G Resilient practical cooperative output regulation for mass with unknown switching exosystem dynamics under dos attacks. *Automatica* 2022;139:110172. DOI
14. 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;51:1345-53. DOI
15. Zhang D, Feng G. A new switched system approach to leader-follower consensus of heterogeneous linear multiagent systems with dos attack. *EEE Trans Syst Man Cybern, Syst* 2021;51:1258-66. DOI
16. Abdollahi Biron Z, Dey S, Pisu P. Real-time detection and estimation of denial of service attack in connected vehicle systems. *IEEE Trans Intell Transport Syst* 2018;19:3893-902. DOI
17. Doostmohammadian M, Meskin N. Finite-time stability under denial of service. *IEEE Syst J* 2021;15:1048-55. DOI
18. Xiao S, Ge X, Han QL, Cao Z, Zhang Y, Wang H. Resilient distributed event-triggered control of vehicle platooning under dos attacks. *IFAC-PapersOnLine* 2020;53:1807-12. DOI
19. Merco R, Ferrante F, Pisu P. A hybrid controller for dos-resilient string-stable vehicle platoons. *IEEE Trans Intell Transport Syst* 2021;22:1697-707. DOI
20. Miao KL, Zhu JW, Zhang WA, Distributed guaranteed cost control of networked interconnected systems under denial-of-service attacks: a switched system approach. In: 2018 33rd Youth Academic Annual Conference of Chinese Association of Automation (YAC); 2018. p. 911-5. DOI
21. Zhang D, Shen Y, Zhou S, Dong X, Yu L. Distributed secure platoon control of connected vehicles subject to dos attack: theory and application. *IIEEE Trans Syst Man Cybern, Syst* 2021;51:7269-78. DOI
22. Sakiz F, Sen S. A survey of attacks and detection mechanisms on intelligent transportation systems: vanets and iov. *Ad Hoc Networks* 2017;61:33-50. DOI
23. Ju Z, Zhang H, Li X, Chen X, Han J, Yang M. A survey on attack detection and resilience for connected and automated vehicles: from vehicle dynamics and control perspective. *IEEE Trans Intell Veh* 2022;7:815-37. DOI
24. Yuan C, Gu Y, Zeng W, Stegagno P. Switching model predictive control of switched linear systems with average dwell time. In: 2020 American Control Conference (ACC); 2020. p. 2888-93 DOI
25. Yu K, Yang H, Tan X, et al. Model predictive control for hybrid electric vehicle platooning using slope information. *IEEE Trans Intell Transport Syst* 2016;17:1894-909. DOI
26. Zheng Y, Li SE, Li K, Borrelli F, Hedrick JK. Distributed model predictive control for heterogeneous vehicle platoons under unidirectional topologies. *IEEE Trans Contr Syst Technol* 2017;25:899-910. DOI
27. 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 Journal of Control* 2016;18:1030-41. DOI
28. Yan M, Ma W, Zuo L, Yang P. Dual-mode distributed model predictive control for platooning of connected vehicles with nonlinear dynamics. *Int J Control Autom Syst* 2019;17:3091-101. DOI
29. Basiri MH, Azad NL, Fischmeister S. Attack resilient heterogeneous vehicle platooning using secure distributed nonlinear model predictive control. In: 2020 28th Mediterranean Conference on Control and Automation (MED); 2020. p.307-12. DOI
30. Chen J, Sun Z, Zhang H. Event-triggering in distributed mpc of decoupled nonlinear systems against dos attacks. In: 2022 IEEE 5th International Conference on Industrial Cyber-Physical Systems (ICPS); 2022. p. 1-6. DOI
31. 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;72:2863-77. DOI
32. Olfati-saber R, Fax JA, Murray RM. Consensus and cooperation in networked multi-agent systems. *Proc IEEE* 2007;95:215-33. DOI
33. 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 Contr Syst Technol* 2020;28:1066-73. DOI
34. Halder K, Montanaro U, Gillam L, Dianati M, Oxtoby D, Mouzakitis A, Fallah S. Distributed controller design for vehicle platooning under packet drop scenario. In: 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC); 2020. p. 1-8. DOI
35. Huang D, Li S, Zhang Z, Liu Y, Mi B. Design and analysis of longitudinal controller for the platoon with time-varying delay. *IEEE Trans Intell Transport Syst* 2022;23:23628-39. DOI

36. Zheng Y, Eben Li S, Wang J, Cao D, Li K. Stability and scalability of homogeneous vehicular platoon: Study on the influence of information flow topologies. *IEEE Trans Intell Transport Syst* 2016;17:14-26. DOI
37. Wu C, Wu L, Liu J, Jiang Z. Active defense-based resilient sliding mode control under denial-of-service attacks. *IEEE Trans Inform Forensic Secur* 2020;15:237-49. DOI
38. Ye Z, Zhang D, Wu Z. Adaptive event-based tracking control of unmanned marine vehicle systems with dos attack. *J Franklin Inst* 2021;358:1915-39. DOI
39. Zhang D, Liu L, Feng G. Consensus of heterogeneous linear multiagent systems subject to aperiodic sampled-data and dos attack. *IEEE Trans Cybern* 019;49:1501-11. DOI
40. De Persis C, Tesi P. Input-to-state stabilizing control under denial-of-service. *IEEE Trans Automat Contr* 2015;60:2930-44. DOI
41. Peng C, Fei M, Tian E, Guan Y. On hold or drop out-of-order packets in networked control systems. *Inform Sciences* 2014;268:436-46. DOI
42. Zhang D, Xu Z, Karimi HR, Wang Q, Yu L. Distributed H_∞ output-feedback control for consensus of heterogeneous linear multiagent systems with aperiodic sampled-data communications. *IEEE Trans Ind Electron* 2018;65:4145-55. DOI
43. Diblík J, Khusainov D, Baštinec J, Sirenko A. Exponential stability of linear discrete systems with constant coefficients and single delay. *Appl Math Lett* 2016;51:68-73. DOI