

Article

Data-Driven Prescribed Performance Platooning Control Under Aperiodic Denial-of-Service Attacks

Peng Zhang ¹, Zhenling Wang ¹ and Weiwei Che ^{2,*}¹ Shandong Key Laboratory of Industrial Control Technology, School of Automation, Qingdao University, Qingdao 266071, China² State Key Laboratory of Synthetical Automation for Process Industries, College of Information Science and Engineering, Northeastern University, Shenyang 110819, China

* Correspondence: cheweiwei@ise.neu.edu.cn

Abstract: This article studies a data-driven prescribed performance platooning control method for nonlinear connected automated vehicle systems (CAVs) under aperiodic denial-of-service (DoS) attacks. Firstly, the dynamic linearization technique is employed to transform the nonlinear CAV system into an equivalent linearized data model. Secondly, to improve the system's transient performance, a prescribed performance transformation (PPT) scheme is proposed to transform the constrained output into the unconstrained one. In addition, an attack compensation mechanism is designed to reduce the adverse impact. Combining the PPT scheme and the attack compensation mechanism, the data-driven adaptive platooning control scheme is proposed to achieve the vehicular tracking control task. Lastly, the merits of the developed control method are illustrated by an actual simulation.

Keywords: model-free adaptive control; connected automated vehicles; prescribed performance control; aperiodic DoS attacks

MSC: 93D25



Citation: Zhang, P.; Wang, Z.; Che, W.. Data-Driven Prescribed Performance Platooning Control Under Aperiodic Denial-of-Service Attacks.

Mathematics **2024**, *12*, 3313. <https://doi.org/10.3390/math12213313>

Academic Editor: António Lopes

Received: 12 September 2024

Revised: 11 October 2024

Accepted: 14 October 2024

Published: 22 October 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

With the improvement and maturity of new generation digital technologies such as artificial intelligence, Internet of Things, and 5G mobile communications, connected automated vehicle systems (CAVs) have become a new trend in the development of the automotive industry. For the purpose of dealing with the adverse impact generated by network attacks and event triggering, the authors of [1] develop a resilient event-triggered controller for CAVs. To reduce the resource consumption and pollution emissions, a hybrid model predictive control scheme for CAVs is developed in [2]. The authors of [3] develop a hierarchical collaborative tracking control strategy for CAVs to reduce traffic throughput and vehicle fuel efficiency in a complex traffic environment. In [4], the authors investigate the cooperative tracking control problem of dynamic event triggering for CAVs with various spacing strategies. To enhance the robustness of the vehicle system, the authors of [5] propose a recent robust control scheme by using an integral sliding mode. With the help of the barrier Lyapunov function, the authors of [6] study the fuzzy adaptive tracking control algorithm for heterogeneous CAVs with input saturation to ensure that collisions do not occur and to maintain communication between vehicles. For a vehicle steer-by-wire system under various parameters, the authors of [7] propose a robust control technique. To ensure collision avoidance and comfort assurance conditions, the authors of [8] propose a hierarchical control approach to address the prescribed performance lane-changing control problem for nonlinear vehicle platoons.

It is worth noting that, in practical applications, CAVs can exchange position and speed information with each other through the communication network. However, the communication network is very fragile and susceptible to cyber attacks, which will cause

the controlled system to be in an unsafe state. In general, the network attacks can be divided into denial-of-service (DoS) attacks and false data injection (FDI) attacks. Differently from an FDI attack, which injects false attack signals into the system, the manner of DoS attacks is to destroy the information transmission channel, i.e., the data of the system cannot be timely transmitted to the controller. Until now, the safety of a vehicle system has been of wide concern [9–14]. The authors of [9] deal with the observer-based security consensus problem under DoS attacks. To deal with arbitrarily large parametric uncertainties, the authors of [10] develop a cooperative robust resilient output regulation control approach for linear uncertain multiagent systems (MASs) under DoS attacks. For mitigating the negative influence of DoS attacks, a novel security tracking control scheme of nonlinear autonomous ground vehicles in [11] is proposed. Due to the interaction information being affected by DoS attacks, the authors of [12] deal with the problem of security cooperative tracking control for nonlinear MASs suffering from DoS attacks. In [13], the authors propose a novel detection method on the basis of the adaptive Kalman filter bank to reduce the effect of FDI attacks. The authors of [14] introduce an adaptive boundary estimation mechanism during the back-stepping controller design process to reduce the adverse influence of FDI attacks. The authors of [15] propose a safe time-varying formation control framework for heterogeneous multiagent systems under the constraints of denial-of-service (DoS) attacks, noncooperative dynamic obstacles, and input saturation.

Although the above results can effectively mitigate the impact of attacks, they are all based on an accurate mathematical model. With the continuous progress of automobile intelligence and electrification, the dynamical modeling of CAVs is becoming more complex. For the purpose of addressing this problem, a model-free adaptive control (MFAC) algorithm is introduced. In the MFAC method [16–19], complex nonlinear systems can be transformed into the equivalent linear data model through applying the dynamic linearization technique (DLT). In addition, the design of a model-free adaptive controller relies merely on the system's input and output information, not the architecture of the system itself. Up to now, the MFAC method has been used in a wide variety of applications, such as MASs [20,21], vehicular platooning systems (VPSs) [22,23], and cyber-physical systems (CPSs) [24]. Through employing the DLT, the authors of [20] develop a novel distributed MFAC strategy for MASs suffering from DoS attacks. In [21], a hierarchical distributed MFAC scheme is introduced to address the cooperative tracking control problem. The authors of [22,23] develop a novel MFAC method for nonlinear VPSs. The authors of [24] address the model-free adaptive tracking control problem for a class of discrete-time single-input single-output nonlinear systems under dynamic sparse attacks and measurement disturbances. Although the security cooperative control problem in the application of the MFAC algorithm has made great achievements, the above papers do not consider the safety problem for nonlinear CAVs under aperiodic DoS attacks. This will be one of the driving forces behind our research in this paper.

On the other hand, the above articles only consider the steady-state performance of the system, but do not consider the transient performance. Nevertheless, the transient performance of the system is also very valuable for the system itself. In an actual vehicular platooning control application, for the purpose of restricting the system's transient performance within the prescribed boundaries and acquire a better tracking control effect, the prescribed performance control (PPC) method is firstly developed in [25] to increase the convergence speed and reduce overshoot. The primary goal of PPC is to limit the error or state of the system to a preset range by applying a strictly increasing function. Until now, the PPC method has gained wide attention [26–28]. Unlike the existing observer-based finite/fixed-time control methods, the authors of [26] develop the observer-based finite-time cooperative tracking control scheme for nonlinear MASs, where the time of convergence and the region of convergence can be pre-specified by the authors. Through the aid of back-stepping technology, the authors of [27] develop a novel adaptive tracking control method. The designed controller is able to guarantee the tracking control performance of the system as well as to reduce the communication burden. The authors of [28] propose a novel model-free path tracking controller that realizes appointed-time performance and reduces the communication burden. Until now, the PPC

method has received great attention in the field of MFAC [29–32]. However, it has been noted that there is a fundamental characteristic of the above control methods that do not take into account the chattering generated by the sliding mode control (SMC) method. To this end, for the chatter problem caused by the SMC method, how to design a novel preset performance-based MFAC method that does not use the SMC scheme, especially for nonlinear CAVs, is a problem worthy of attention of this paper.

Enlightened by the previous discussions, this paper develops a data-driven prescribed performance platooning control strategy under aperiodic DoS attacks. Our major contributions in this articles are described below:

- (1) For nonlinear connected automated vehicle system (CAVs) under state constraint and aperiodic DoS attacks, the nonlinear CAV is converted into an equivalent linear data model by using the dynamic linearization technique (DLT). Moreover, to reduce the adverse effect of aperiodic DoS attacks, an attack compensation mechanism based on the latest received data is proposed, which greatly ensures the safe driving of nonlinear CAVs.
- (2) The existing data-driven prescribed performance platooning control methods [29–32] are based on the sliding mode control framework, which may cause chattering problems. Differently from them, a novel prescribed performance transformation strategy for nonlinear CAVs under aperiodic DoS attacks is developed to complete the vehicular tracking control task.

The rest of this paper is set out in the following. Firstly, the preliminaries and data-driven control algorithm design are shown in Section 2. In Section 3, we present the stability analysis of this paper. Then, the simulation description is presented in Section 4. Ultimately, our conclusion is illustrated in Section 5. To be more clear, Figure 1 is developed to describe each section of this article.

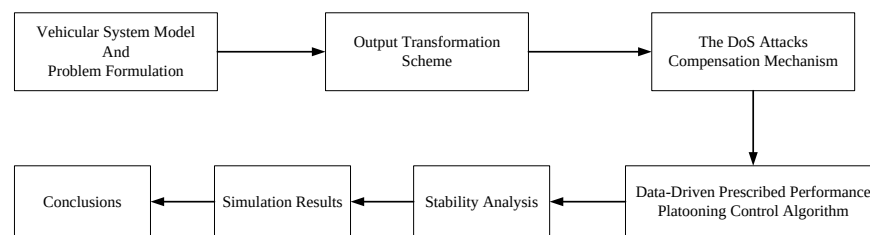


Figure 1. The general block diagram.

2. Preliminaries and Data-Driven Control Algorithm Design

2.1. Connected Automated Vehicle System Model

In this paper, we consider $N + 1$ connected automated vehicle systems (CAVs) driving in a platoon, which is made up of N follower vehicles and one leader vehicle; here, the dynamics model of the i th follower vehicle is defined as the following expression:

$$\begin{aligned} s_i(k+1) &= s_i(k) + T\vartheta_i(k) + \frac{1}{2}T^2(u_i(k) - F_i(k)), \\ \vartheta_i(k+1) &= \vartheta_i(k) + T(u_i(k) - F_i(k)), \end{aligned} \quad (1)$$

where T indicates the sampling time. Moreover, $s_i(k)$, $\vartheta_i(k)$, and $u_i(k)$ with $i = \{1, 2, \dots, N\}$ represent the position, speed, and the pulling/braking power of the i th follower vehicle, respectively. In addition, $F_i(k)$ is a nonlinear drag function that includes two terms, namely, a basis function $f_i^\vartheta(\vartheta_i(k))$ associated with velocity and an additional function $f_i^s(s_i(k))$ related to the position. Here, the specific forms of $f_i^\vartheta(\vartheta_i(k))$ and $f_i^s(s_i(k))$ are defined as the following two equations, respectively:

$$\begin{aligned} f_i^\vartheta(\vartheta_i(k)) &= p_0(k) + p_1(k)\vartheta_i(k) + p_2(k)\vartheta_i^2(k) \\ f_i^s(s_i(k)) &= q_r(s_i(k)) + q_c(s_i(k)) + q_t(s_i(k)) \end{aligned} \quad (2)$$

with $p_0(k)$, $p_1(k)$, and $p_2(k)$ denoting the time-varying drag coefficients. Meantime, $q_r(\cdot)$, $q_c(\cdot)$, and $q_t(\cdot)$ represent the drag relation to ramps, curves, and tunnels, respectively.

Combining (1) with (2), it is possible to obtain

$$s_i(k+1) = s_i(k) + T\vartheta_i(k-1) + T^2u_i(k-1) + \frac{1}{2}T^2u_i(k) - T^2F_{i1}(k-1) - \frac{1}{2}F_{i2}(k), \quad (3)$$

where $F_{i1}(k-1) = p_0(k-1) + p_1(k-1)\vartheta_i(k-1) + p_2(k-1)\vartheta_i^2(k-1) + q_r(s_i(k-1)) + q_c(s_i(k-1)) + q_t(s_i(k-1))$, and $F_{i2}(k) = p_0(k) + p_1(k)\vartheta_i(k) + p_2(k)\vartheta_i^2(k) + q_r(s_i(k)) + q_c(s_i(k)) + q_t(s_i(k))$.

Correspondingly, the leader vehicle is able to be modeled in such a way that

$$\begin{aligned} s_0(k+1) &= s_0(k) + T\vartheta_0(k) \\ \vartheta_0(k+1) &= \vartheta_0(k) + TF_0(k) \end{aligned} \quad (4)$$

with $s_0(k)$ and $\vartheta_0(k)$ indicating the vehicular position and speed of leader. $F_0(k)$ denotes the nonlinear function.

It can be acquired from (3) that $s_i(k+1) = f_i(k)$, in which $f_i(\cdot)$ denotes an unknown nonlinear function, containing the speeds $\vartheta_i(k)$, $\vartheta_i(k-1)$, positions $s_i(k)$, $s_i(k-1)$, and control inputs $u_i(k)$, $u_i(k-1)$.

The nonlinear function $f_i(k)$ of CAVs is able to be transformed to an equivalent linear data model with the CFDL technique through making the following assumptions about the nonlinear CAVs (1).

Assumption 1 ([16]). For unknown nonlinear function $f_i(\cdot)$, the partial derivative of the nonlinear function $f_i(\cdot)$ in relation to the control input $u_i(k)$ is continuous.

Assumption 2 ([18]). Nonlinear CAVs (1) and (4) meet the generalized Lipschitz condition, namely, when $\Delta u_i(k) \neq 0$, then one can know that $|\Delta s_i(k+1)| \leq \tilde{\beta}_i |\Delta u_i(k)|$ holds, in which $\Delta u_i(k) = u_i(k) - u_i(k-1)$, $\Delta s_i(k+1) = s_i(k+1) - s_i(k)$, and $\tilde{\beta}_i > 0$ represents a constant.

Assumption 3 ([16]). From the perspective of realistic application, the system output increment $\Delta s_0(k)$ of the leader vehicle is supposed to be bounded, i.e., $|\Delta s_0(k)| \leq \varrho_1$ with $\varrho_1 > 0$ being a constant, where $\Delta s_0(k) = s_0(k) - s_0(k-1)$.

Remark 1. Assumption 1 represents a basic restrictive condition employed in the nonlinear system [18–20]. Assumption 2 is used to illustrate the correlation between the system's input and output increments.

Lemma 1 ([16]). For nonlinear CAVs, if Assumptions 1 and 2 can be satisfied, and $\Delta u_i(k) \neq 0$, then there exists a pseudo partial derivative (PPD) parameter that converts the nonlinear CAVs (1) to the form of the following input and output increments:

$$\Delta s_i(k+1) = \psi_i^s(k) \Delta u_i(k), \quad (5)$$

where $\psi_i^s(k)$ denotes a time-varying and bounded PPD parameter, which satisfies $|\psi_i^s(k)| \leq \bar{c}_i$.

Remark 2. In Lemma 1, we give the connection between the controller input increment and the output increment, that is to say, the output of CAVs changes identically with the input to CAVs. With the assistance of this one feature, in the following controller design, we use only the input and output information from the nonlinear CAVs.

2.2. Prescribed Performance Control Scheme Design

During the actual vehicle movement, the steady-state and transient performance of nonlinear CAVs play a key role. Here, for the purpose of ensuring the transient performance of nonlinear CAVs and achieve a preset performance under preset conditions, a prescribed performance transformation scheme is shown in this subsection. First of all, the position tracking error of nonlinear CAVs is designed as the following expression:

$$e_i(k) = s_0(k) - s_i(k) - d_{i,0}, \quad (6)$$

where $d_{i,0}$ indicates the desired security distance between the i th follower and leader. Moreover, from Assumption 3, one can assume that $|s_0(k)| \leq \bar{s}_0$.

For the output of nonlinear CAVs, the prescribed performance transformed scheme is developed as follows:

$$-\Pi_i(k) < s_i(k) < \Pi_i(k), \quad (7)$$

where $\Pi_i(k)$ denotes the prescribed performance function.

Here, its specific expression is designed in the following form:

$$\begin{aligned} \Pi_i(k+1) &= (1 - \kappa_i)\Pi_i(k) + \kappa_i\Pi_i(\infty), \\ \lim_{k \rightarrow \infty} \Pi_i(k) &= \Pi_i(\infty), \end{aligned} \quad (8)$$

where the initial state of $\Pi_i(0)$ satisfies $|\Pi_i(0)| > |\Pi_i(\infty)| > 0$. $\kappa_i \in (0, 1)$ represents the convergent rate.

For the purpose of ensuring that the tracking error $e_i(k)$ of vehicular position is capable of converging to the preset region, the following prescribed performance control scheme is formulated from (6) and (7):

$$-\Pi_i(k) - \bar{s}_0 + d_{i,0} < e_i(k) < \Pi_i(k) + \bar{s}_0 - d_{i,0}. \quad (9)$$

With a view to minimizing the complexity of the controller design process and strengthen the transient performance of the nonlinear CAVs, the strictly increasing function $Y(\delta_i(k))$ is able to be introduced to deal with the restricted vehicular tracking control problem (7). To this end, the output signal $s_i(k)$ is converted into the unconstrained one $\delta_i(k)$, namely,

$$s_i(k) = \Pi_i(k)Y(\delta_i(k)) \quad (10)$$

with $Y(\delta_i(k))$ satisfying the following properties:

- (i) $Y(\delta_i(k)) \in (-1, 1)$ for any $\delta_i(k)$;
- (ii) $\lim_{k \rightarrow +\infty} Y(\delta_i(k)) = 1$, and $\lim_{k \rightarrow -\infty} Y(\delta_i(k)) = -1$.

In general, $Y(\delta_i(k))$ associated with $\delta_i(k)$ is designed as

$$Y(\delta_i(k)) = \frac{e^{\delta_i(k)} - e^{-\delta_i(k)}}{e^{\delta_i(k)} + e^{-\delta_i(k)}}. \quad (11)$$

Then, the following equation can be acquired from (11):

$$\delta_i(k) = \frac{1}{2} \ln \left(\frac{\Pi_i(k) + s_i(k)}{\Pi_i(k) - s_i(k)} \right). \quad (12)$$

Remark 3. It is noteworthy that the constrained output $s_i(k)$ can be converted into the unconstrained one through employing the strictly increasing function $Y(\delta_i(k))$. In addition, by adjusting the prescribed region, the position tracking error is also able to converge to the prescribed region (9), which significantly increases the transient performance of nonlinear CAVs.

Substituting $s_i(k+1) = f_i(k)$ into (12) yields

$$\delta_i(k+1) = \frac{1}{2} \ln \left(\frac{\Pi_i(k) + f_i(k)}{\Pi_i(k) - f_i(k)} \right), \quad (13)$$

here, $f_i(k) = f_i(s_i(k), \vartheta_i(k), u_i(k))$.

By analyzing (13), one can know that $\delta_i(k+1)$ denotes a nonlinear function related to the position $s_i(k)$, speed $\vartheta_i(k)$, control input $u_i(k)$, and prescribed performance function $\Pi_i(k)$. Therefore, the new nonlinear function can be redeveloped as $\Phi(\cdot)$, i.e., $\delta_i(k+1) = \Phi_i[s_i(k), \vartheta_i(k), u_i(k), \Pi_i(k)]$.

Lemma 2 ([20]). *Through using the homeomorphism mapping method, one can know that $\delta_i(k)$ is the unconstrained output generated by the constrained output $s_i(k)$, namely, if Assumptions 1 and 2 hold, and $\Delta u_i(k) \neq 0$, there exists a PPD parameter that allows the unconstrained output $\delta_i(k)$ to be represented as the unconstrained linear data model below:*

$$\Delta \delta_i(k+1) = \varphi_i(k) \Delta u_i(k), \quad (14)$$

where $|\varphi_i(k)| \leq \varphi_s^*$ with $\varphi_s^* > 0$ being a constant. $\Delta \delta_i(k+1) = \delta_i(k+1) - \delta_i(k)$.

Remark 4. *The existing adaptive control schemes include virtual reference feedback tuning, iterative feedback tuning, and unfalsified control, which either require precise information about the system model or ignore, to varying degrees, the effect of linearization of the nonlinear function on the controller design. Differently from them, the model-free adaptive control method has a simple structure, moderate adjustable parameters, easy controller design, and direct use of system input and output data.*

One thing worth noting is that it is quite difficult to obtain the real value of $\varphi_i(k)$. To this end, the performance function is defined as the following expression:

$$J[\hat{\varphi}_i(k)] = |\Delta \delta_i(k) - \hat{\varphi}_i(k) \Delta u_i(k-1)|^2 + \eta_i |\hat{\varphi}_i(k) - \hat{\varphi}_i(k-1)|^2 \quad (15)$$

with $\eta_i > 0$ denoting the penalty factor.

Further, the following PPD parameter estimation algorithm can be acquired through minimizing the above performance function (15):

$$\hat{\varphi}_i(k) = \hat{\varphi}_i(k-1) + \frac{\rho_i \Delta u_i(k-1) [\Delta \delta_i(k) - \hat{\varphi}_i(k-1) \Delta u_i(k-1)]}{\Delta u_i^2(k-1) + \eta_i} \quad (16)$$

with $\rho_i \in [0, 1)$ denoting the step-size factor.

For the purpose of optimizing system performance, the performance function is described as the following expression:

$$J[u_i(k)] = |\delta_0(k) - d_{i,0} - \delta_i(k) - \hat{\varphi}_i(k) \Delta u_i(k)|^2 + \lambda_i |\Delta u_i(k)|^2, \quad (17)$$

where $\delta_0(k)$ is the transformed output of the leader.

Similar to the solution of (16), the following formula can be acquired from (17) that

$$u_i(k) = u_i(k-1) + \frac{\tau_i \hat{\varphi}_i(k) [\delta_0(k) - d_{i,0} - \delta_i(k)]}{\hat{\varphi}_i^2(k) + \lambda_i}, \quad (18)$$

where the effects of τ_i and λ_i are the same as ρ_i and η_i .

2.3. Data-Driven Prescribed Performance Platooning Control under Aperiodic DoS Attacks

The designed data-driven platooning control scheme of nonlinear CAVs is presented in Figure 2. From observation of Figure 2, it can be derived that the prescribed performance function $P_i(k)$ is introduced here to guarantee the system's transient performance. Then,

we can observe that the information $[\delta_i(k), \hat{\phi}_i(k)]$ can be transmitted between the sensor and controller through the vehicle interaction network. Once the attacker launches the attack, the controller is unable to acquire the data from the sensor. An illustration of an aperiodic DoS attack is displayed in Figure 3. Here, $T_i^s \in \mathbb{N}$ and $T_i^e \in \mathbb{N}$ are introduced to show the beginning and the ending moment of the i th attack, respectively. Additionally, the red area is used to indicate that the system is attacked, and the green area is used to indicate that the system is not attacked at this time.

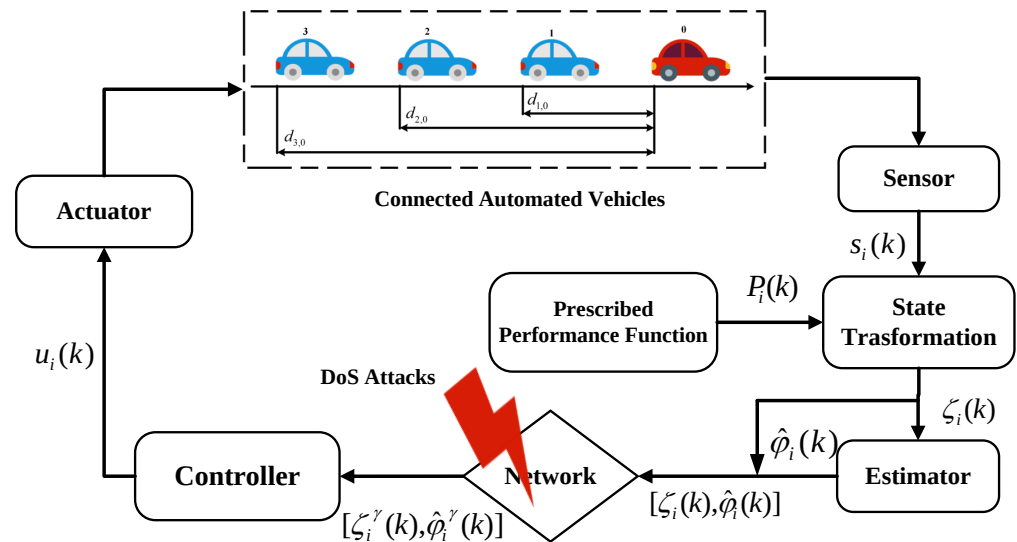


Figure 2. System block diagram of the data-driven platooning control scheme.

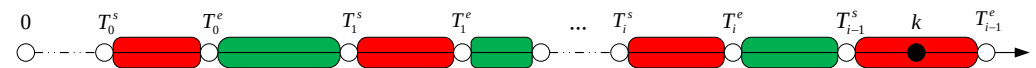


Figure 3. Illustration of aperiodic DoS attack.

Moreover, to verify whether the attack occurs, the DoS attack indicator function $q_i(k)$ is developed; the specific expression is designed as follows:

$$q_i(k) = \begin{cases} 1, & k \in [T_{i-1}^e, T_i^s), \\ 0, & k \in [T_i^s, T_i^e), \end{cases} \quad (19)$$

where $[T_i^s, T_i^e)$, and $[T_{i-1}^e, T_i^s)$ represent the i th attack period and attack dormant interval. Based on which, the collection of all attack intervals in $[0, k]$ can be described as follows:

$$\Lambda_a(0, k) = \left\{ \bigcup_{i \in N} [T_i^s, T_i^e) \right\} \cap [0, k]. \quad (20)$$

Moreover, the interval of no DoS attacks can be represented by

$$\Lambda_b(0, k) = [0, k] / \Lambda_a(0, k), \quad (21)$$

where $[0, k] / \Lambda_a(0, k)$ represents a set which contains the set $[0, k]$ and does not contain the set $\Lambda_a(0, k)$.

Assumption 4 ([33]). $\Lambda_a(0, k)$ satisfies the following condition:

$$|\Lambda_a(0, k)| \leq \Lambda_0 + \frac{k}{\epsilon}, \quad (22)$$

where Λ_0 indicates the original attack period parameter, which is used to deal with the situation where the CAV is attacked from the beginning. $\epsilon > 1$ denotes the attack interval coefficient that needs to be designed later.

According to (19), the following attack mechanism can be acquired:

$$\begin{aligned}\delta_i^o(k) &= \varrho_i(k)\delta_i(k) + (1 - \varrho_i(k))\delta_i^o(k-1), \\ \hat{\varphi}_i^o(k) &= \varrho_i(k)\hat{\varphi}_i(k) + (1 - \varrho_i(k))\hat{\varphi}_i^o(k-1).\end{aligned}\quad (23)$$

According to (16) and (18), and the attack compensation mechanism (22), the prescribed performance-based MFAC scheme for nonlinear CAVs with aperiodic DoS attacks is designed as follows:

$$\begin{aligned}\hat{\varphi}_i(k) &= \hat{\varphi}_i(k-1) + \varrho_i(k)\Delta u_i(k-1) \\ &\quad \times \frac{\rho_i[\Delta\delta_i(k) - \hat{\varphi}_i(k-1)\Delta u_i(k-1)]}{\Delta u_i^2(k-1) + \eta_i},\end{aligned}\quad (24a)$$

$$\begin{aligned}\hat{\varphi}_i(k) &= \hat{\varphi}_i(1), \text{ if } |\hat{\varphi}_i(k)| \leq \iota_i, \text{ or } |\Delta u_i(k-1)| \leq \iota_i \\ &\quad \text{or } \text{sign}(\hat{\varphi}_i(k)) \neq \text{sign}(\hat{\varphi}_i(1)),\end{aligned}\quad (24b)$$

$$u_i(k) = u_i(k-1) + \frac{\tau_i \hat{\varphi}_i^o(k)[\delta_0(k) - d_{i,0} - \delta_i^o(k)]}{\hat{\varphi}_i^o(k)^2 + \lambda_i}, \quad (25)$$

where ι_i represents an arbitrarily small positive constant.

Remark 5. It can be acquired that (24b) represents the reset condition of the estimation PPD parameter $\hat{\varphi}_i(k)$, which means the efficiency and feasibility of the PPD parameter estimation algorithm (24a) can be improved.

Remark 6. The existing prescribed performance-based data-driven control method [29–31], through constructing the sliding mode function, may cause the chattering problem. To deal with this problem, the prescribed performance function $\Pi_i(k)$ of this paper is directly used in the cost functions (15) and (17), based on which, the position tracking error of CAVs can converge to the preset region.

Problem 1. For nonlinear CAVs (1), the objective of this article is to propose a prescribed performance-based MFAC strategy consisting of (24a)–(25) subject to aperiodic DoS attacks to guarantee the transformed output $\delta_i(k)$ is uniformly ultimately bounded. Mathematically, it is capable of converging to the following set, i.e., $\{\delta_i(k) | \lim_{k \rightarrow \infty} |\delta_i(k)| \leq \delta^*\}$.

3. Stability Analysis

In this part, our main purpose is to analyze the stability of CAVs. In order to present more clearly the control scheme designed in this paper, the whole control algorithm is shown in Algorithm 1.

Algorithm 1 Data-Driven Prescribed Performance Resilient Control Algorithm.

- 1: Select suitable parameters τ_i , λ_i , ρ_i , η_i , ϵ_1 , and ϵ_2 .
 - 2: The system's state is constrained within the prescribed region (7).
 - 3: The constrained state is converted into the unconstrained one (12).
 - 4: The attack compensation mechanism (23) is designed to reduce the impact of attacks.
 - 5: Updating $\hat{\varphi}_i(k)$ by using estimation algorithm (24a) and (24b).
 - 6: Verify the reset conditions:
if $|\hat{\varphi}_i(k)| < \iota_i$ or $|\Delta u_i(k-1)| < \iota_i$ or $\text{sign}(\hat{\varphi}_i(k)) \neq \text{sign}(\hat{\varphi}_i(1))$, then $\hat{\varphi}_i(k) = \hat{\varphi}_i(1)$.
 - 7: Input leader $\delta_0(k)$, safety distance $d_{i,0}$, and compensation mechanism $\hat{\varphi}_i^o(k)$ and $\delta_i^o(k)$.
 - 8: Update the control input $u_i(k)$ with (25) and output it.
-

The major theorem of this article is presented as follows.

Theorem 1. In accordance with Assumptions 1–4, Problem 1 can be addressed with the developed prescribed performance-based model-free adaptive resilient control algorithm subject to aperiodic DoS attacks made of (24a)–(25), if the parameters are chosen to meet $\tau_i \in [0, 1)$, $\lambda_i > \lambda_{\min} > 0$ with $\lambda_{\min} = (\frac{\varphi_s^*}{2})^2$, $\rho_i \in [0, 1)$, $\eta_i > 0$, $\varepsilon_1 \in (0, 1)$, $\varepsilon_2 > 1$, and

$$1 < \epsilon < \frac{\ln \varepsilon_1 - \ln \varepsilon_2}{\ln \varepsilon_1}. \quad (26)$$

Proof. Throughout this segment, we will conduct the stability proofs, in which the proofs can be separated into the proceeding two main aspects: (i) proving the boundedness of estimation error of PPD parameter $e_{\varphi_i}(k)$; (ii) proving that the converted output $\delta_i(k)$ is bounded.

Part I: In the first place, the estimation error of the PPD parameter is defined as $e_{\varphi_i}(k) = \hat{\varphi}_i(k) - \varphi_i(k)$. Through subtracting $\varphi_i(k)$ on both sides of (24a), it is possible to acquire

$$\begin{aligned} e_{\varphi_i}(k) &= \hat{\varphi}_i(k-1) - \varphi_i(k) + \Delta u_i(k-1) \\ &\quad \times \frac{\rho_i[\Delta \delta_i(k) - \hat{\varphi}_i(k-1)\Delta u_i(k-1)]}{\Delta u_i^2(k-1) + \eta_i} \\ &= \left(1 - \frac{\rho_i \Delta u_i^2(k-1)}{\Delta u_i^2(k-1) + \eta_i}\right) e_{\varphi_i}(k-1) \\ &\quad + \varphi_i(k-1) - \varphi_i(k). \end{aligned} \quad (27)$$

Taking absolute values for both sides of the above (27), the following expression can be acquired:

$$\begin{aligned} |e_{\varphi_i}(k)| &\leq \left|1 - \frac{\rho_i \Delta u_i^2(k-1)}{\Delta u_i^2(k-1) + \eta_i}\right| |e_{\varphi_i}(k-1)| \\ &\quad + |\varphi_i(k-1) - \varphi_i(k)|. \end{aligned} \quad (28)$$

In addition, according to the reset condition (24b), one can obtain the minimum value of $\frac{\rho_i \Delta u_i^2(k-1)}{\Delta u_i^2(k-1) + \eta_i}$ is $\frac{\rho_i \iota_i^2}{\eta_i + \iota_i^2}$. Based on this, one can obtain

$$\left|1 - \frac{\rho_i \Delta u_i^2(k-1)}{\Delta u_i^2(k-1) + \eta_i}\right| \leq 1 - \frac{\rho_i \iota_i^2}{\eta_i + \iota_i^2} \triangleq \theta_i < 1. \quad (29)$$

Then, taking into account that the boundedness of $\varphi_i(k)$ has been given in Lemma 2, it is possible to infer that $|\varphi_i(k-1) - \varphi_i(k)| \leq 2\varphi_s^*$.

Furthermore, considering these points, Equation (28) can be redeveloped as follows:

$$\begin{aligned} |e_{\varphi_i}(k)| &\leq \theta_i |e_{\varphi_i}(k-1)| + 2\varphi_s^* \\ &\leq \theta_i^2 |e_{\varphi_i}(k-2)| + 2\varphi_s^* (\theta_i + 1) \\ &\leq \dots \\ &\leq \theta_i^{k-1} |e_{\varphi_i}(1)| + \frac{2\varphi_s^* (1 - \theta_i^{k-1})}{1 - \theta_i}. \end{aligned} \quad (30)$$

Therefore, according to (28)–(30), we can know that the boundedness of estimation error $e_{\varphi_i}(k)$ can be guaranteed. Further, dependent on the description of estimation error $e_{\varphi_i}(k) = \hat{\varphi}_i(k) - \varphi_i(k)$, we are capable of acquiring that $\hat{\varphi}_i(k)$ is ultimately uniformly bounded.

Part II: In this part, we will verify the transformed output $\delta_i(k)$ is ultimately uniformly bounded. In the first place, the transformed tracking error $e_{\delta_i}(k)$ is determined in such a form that

$$e_{\delta_i}(k) = \delta_0(k) - \delta_i(k) - d_{i,0}. \quad (31)$$

According to the characteristics of aperiodic DoS, we will prove from the attack interval and non-attack interval, respectively.

- (1) When $k \in [T_{i-1}^e, T_i^s)$ and $\varrho_i(k) = 1$, namely, the communication channel between the sensor and the controller is not subject to DoS attacks. On account of (14), (25), and (31), we can obtain

$$\begin{aligned} e_{\delta i}(k+1) &= \delta_0(k+1) - \delta_i(k) - \varphi_i(k)\Delta u_i(k) - d_{i,0} \\ &= \Delta\delta_0(k+1) + e_{\delta i}(k) - \frac{\tau_i\varphi_i(k)\hat{\varphi}_i(k)}{\lambda_i + \hat{\varphi}_i^2(k)}e_{\delta i}(k) \\ &= \left(1 - \frac{\tau_i\varphi_i(k)\hat{\varphi}_i(k)}{\lambda_i + \hat{\varphi}_i^2(k)}\right)e_{\delta i}(k) + \Delta\delta_0(k+1). \end{aligned} \quad (32)$$

Then, taking the absolute value on both sides of (32), it is possible to obtain that

$$|e_{\delta i}(k+1)| \leq \left|1 - \frac{\tau_i\varphi_i(k)\hat{\varphi}_i(k)}{\lambda_i + \hat{\varphi}_i^2(k)}\right| + |\Delta\delta_0(k+1)|. \quad (33)$$

According to the conditions given in Theorem 1 and Lemma 2, one can acquire that $\tau_i \in [0, 1)$, $\lambda_i > \lambda_{\min} > 0$ with $\lambda_{\min} = (\frac{\varphi_s^*}{2})^2$, and $|\varphi_i(k)| \leq \varphi_s^*$. Based on this, the following inequality can hold:

$$0 < H_i < \left|\frac{\tau_i\varphi_i(k)\hat{\varphi}_i(k)}{\lambda_i + \hat{\varphi}_i^2(k)}\right| < \left|\frac{\tau_i\varphi_s^*\hat{\varphi}_i(k)}{2\sqrt{\lambda_i}\hat{\varphi}_i(k)}\right| < \frac{\tau_i\varphi_s^*}{2\sqrt{\lambda_i}} = \tau_i < 1. \quad (34)$$

Further, it yields

$$0 < \left|1 - \frac{\tau_i\varphi_i(k)\hat{\varphi}_i(k)}{\lambda_i + \hat{\varphi}_i^2(k)}\right| < 1 - H_i \triangleq \omega_1 < 1. \quad (35)$$

Furthermore, it follows from (35) that

$$|e_{\delta i}(k+1)| < \omega_1|e_{\delta i}(k)| + \varrho_1, \quad (36)$$

where $|\Delta\delta_0(k+1)| \leq \varrho_1$, in which the boundedness of $\Delta\delta_0(k+1)$ has been given in Assumption 3.

- (2) When $k \in [T_i^s, T_i^e)$ and $\varrho_i(k) = 0$, namely, there exist DoS attacks.

According to (31), the following equation is capable of being acquired:

$$e_{\delta i}(k+1) = \Delta\delta_0(k+1) + e_{\delta i}(k) - \varphi_i(k)\Delta u_i(k). \quad (37)$$

In addition, through taking absolute values for both sides of the above (37), it can be acquired that

$$|e_{\delta i}(k+1)| < |e_{\delta i}(k)| + |\Omega_i(k)|, \quad (38)$$

where $\Omega_i(k) = \Delta\delta_0(k+1) - \varphi_i(k)\Delta u_i(k)$.

Taking into account the practical limitations of the physical structure of the vehicle, it is impossible to change the actuator too fast in actual application [22,23]. Based on this situation, the controller input increment is supposed to be bounded [34], namely, $|\Delta u_i(k)| \leq \bar{b}_i$ with $\bar{b}_i > 0$ being a constant. Moreover, the boundedness of $\Delta\delta_i(k+1)$ and $\varphi_i(k)$ has already been given before. To this end, it is possible to acquire that $\Omega_i(k)$ is bounded, namely, $|\Omega_i(k)| \leq \varrho_2$ with $\varrho_2 > 0$ being a constant.

On the basis of the above analysis, Equation (38) has been redesigned in the following form:

$$|e_{\delta i}(k+1)| < \omega_2|e_{\delta i}(k)| + \varrho_2, \quad (39)$$

where $\omega_2 > 1$.

According to (36) and (39), and the aperiodic DoS attack compensation mechanism, it is yielded that

$$|e_{\delta i}(k+1)| < \begin{cases} \omega_1 |e_{\delta i}(k)| + \varrho_1, & k \in [T_{i-1}^e, T_i^s), \\ \omega_2 |e_{\delta i}(k)| + \varrho_2, & k \in [T_i^s, T_i^e). \end{cases} \quad (40)$$

One thing worth noting is that there exist two situations for arbitrary time k , namely, $k \in [T_{i-1}^e, T_i^s)$ and $k \in [T_i^s, T_i^e)$. We assume that, when $k \in [T_i^s, T_i^e)$, the following specific derivation is capable of being obtained:

$$\begin{aligned} |e_{\delta i}(k+1)| &< \omega_2 |e_{\delta i}(k)| + \varrho_2 \\ &< \omega_2^2 |e_{\delta i}(k-1)| + \omega_2 \varrho_2 + \varrho_2 \\ &< \dots \\ &< \omega_2^{k-T_i^s+1} |e_{\delta i}(T_i^s)| + \sum_{n=0}^{k-T_i^s} \omega_2^n \varrho_2 \\ &< \omega_2^{k-T_i^s+1} (\omega_1 |e_{\delta i}(T_i^s-1)| + \varrho_1) \\ &\quad + \sum_{n=0}^{k-T_i^s} \omega_2^n \varrho_2 \\ &< \omega_2^{k-T_i^s+1} (\omega_1^2 |e_{\delta i}(T_i^s-2)| + \omega_1 \varrho_1 + \varrho_1) + \sum_{n=0}^{k-T_i^s} \omega_2^n \varrho_2 \\ &< \dots \\ &< \omega_2^{k-T_i^s+1} \omega_1^{T_i^s-T_{i-1}^e} |e_{\delta i}(T_{i-1}^e)| + \sum_{n=0}^{k-T_i^s} \omega_2^n \varrho_2 \\ &\quad + \omega_2^{k-T_i^s+1} \sum_{n=0}^{T_i^s-T_{i-1}^e-1} \omega_1^n \varrho_1 \\ &< \dots \\ &< \omega_1^{|\Lambda_b(0,k)|} \omega_2^{|\Lambda_a(0,k)|} |e_{\delta i}(0)| + \sum_{n=1}^k \omega_1^{k-n} \\ &\quad \times \omega_1^{-|\Lambda_a(n,k)|} \omega_2^{|\Lambda_a(n,k)|} \varrho_s \end{aligned} \quad (41)$$

with $\varrho_s = \max\{\varrho_1, \varrho_2\}$.

Moreover, when $k \in [T_{i-1}^e, T_i^s)$, we can obtain the same results. In addition, according to (20)–(22), one can acquire that $|\Lambda_b(0,k)| = k - |\Lambda_a(0,k)|$ and $|\Lambda_a(0,k)| \leq \Lambda_0 + \frac{k}{\epsilon}$. Based on this, the following inequality can be acquired:

$$\begin{aligned} |e_{\delta i}(k+1)| &< \omega_1^{k-|\Lambda_a(0,k)|} \omega_2^{|\Lambda_a(0,k)|} |e_{\delta i}(0)| + \sum_{n=1}^k \omega_1^{k-n} \\ &\quad \times \omega_1^{-|\Lambda_a(n,k)|} \omega_2^{|\Lambda_a(n,k)|} \varrho_s \\ &\leq e^{(k-|\Lambda_a(0,k)|) \ln \omega_1 + |\Lambda_a(0,k)| \ln \omega_2} |e_{\delta i}(0)| \\ &\quad + \sum_{n=1}^k e^{(k-n-|\Lambda_a(0,k)|) \ln \omega_1 + |\Lambda_a(n,k)| \ln \omega_2} \varrho_s \\ &\leq e^{(k-\Lambda_0-\frac{k}{\epsilon}) \ln \omega_1 + (\Lambda_0+\frac{k}{\epsilon}) \ln \omega_2} |e_{\delta i}(0)| \\ &\quad + \sum_{n=1}^k e^{(k-n-\Lambda_0-\frac{k-n}{\epsilon}) \ln \omega_1 + (\Lambda_0+\frac{k-n}{\epsilon}) \ln \omega_2} \varrho_s \\ &\leq e^{(\ln \omega_2 - \ln \omega_1) \Lambda_0 + [\ln \omega_1 + \frac{1}{\epsilon} (\ln \omega_2 - \ln \omega_1)] k} |e_{\delta i}(0)| \\ &\quad + \sum_{n=1}^k e^{(\ln \omega_2 - \ln \omega_1) \Lambda_0 + [\ln \omega_1 + \frac{1}{\epsilon} (\ln \omega_2 - \ln \omega_1)] (k-n)} \varrho_s \\ &\leq e^{(\ln \omega_2 - \ln \omega_1) \Lambda_0} e^{[\ln \omega_1 + \frac{1}{\epsilon} (\ln \omega_2 - \ln \omega_1)] k} |e_{\delta i}(0)| \\ &\quad + e^{(\ln \omega_2 - \ln \omega_1) \Lambda_0} \varrho_s \\ &\quad \times \sum_{n=1}^k e^{[\ln \omega_1 + \frac{1}{\epsilon} (\ln \omega_2 - \ln \omega_1)] (k-n)}. \end{aligned} \quad (42)$$

According to condition (26) presented in (1), one can obtain that $\ln \omega_1 + \frac{1}{\epsilon}(\ln \omega_2 - \ln \omega_1) < 0$. Based on this, it follows (42) that the tracking error $e_{\delta_i}(k)$ can be shown to be uniformly bounded, i.e., $e_{\delta_i}(k)$ is capable of converging to the following set: $\{e_{\delta_i}(k) | |e_{\delta_i}(k)| \leq e^{(\ln \omega_2 - \ln \omega_1)\Lambda_0}(|e_{\delta_i}(k)| + \varrho_s)\}$.

Depending on the principle of homeomorphism mapping, the constrained output $-\Pi_i(k) < s_i(k) < \Pi_i(k)$ can be transformed into the unconstrained one $\delta_i(k)$. In addition, in accordance with the boundedness of $e_{\delta_i}(k)$ and $\delta_0(k)$, one can conclude that the transformed output $\delta_i(k)$ is bounded. Furthermore, the boundedness of the constrained output $s_i(k)$ and tracking error $e_i(k)$ can be ensured through proving the converted output $\delta_i(k)$ is bounded. $\square$

Remark 7. In [35], the authors propose a new gain adaptation law for a discrete-time sliding mode. This method relaxes the assumption of a known bound and can tackle the uncertainty without any knowledge of the bound of uncertainty while overcoming the over- and under-estimation problems of switching gain. This method is worth learning and following and will be used in our future work.

4. Simulation

In this segment, the designed preset performance-based model-free adaptive tracking control method of nonlinear CAVs subject to aperiodic DoS attacks is illustrated by a real-world simulation example.

The actual connected automated vehicle system is shown in Figure 4, which consists of three followers and one leader. Further, the dynamics model of the leader is designed as

$$\begin{aligned} s_0(k+1) &= s_0(k) + Tv_0(k), \\ \vartheta_0(k+1) &= 2 + \frac{3.3}{1 + e^{-0.0008k+5}}. \end{aligned}$$

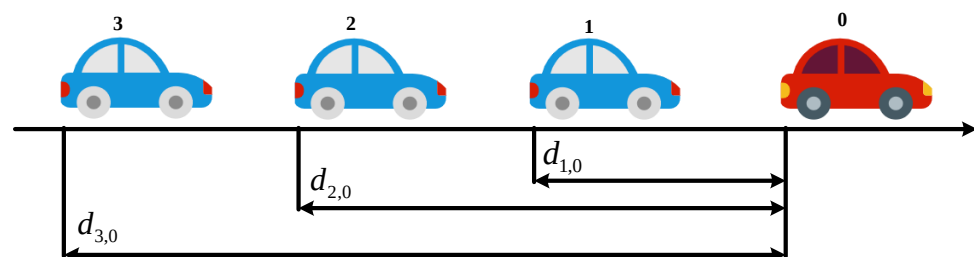


Figure 4. The connected automated vehicle systems.

The position dynamics of the follower vehicle is designed as follows [23]:

$$\begin{aligned} s_i(k+1) &= s_i(k) + T\vartheta_i(k) + 1/2T^2(u_i(k) - 1.2 \times 10^{-4}\vartheta_i(k) \\ &\quad - 2.4 \times 10^{-6}\vartheta_i(k)^2 - 3\vartheta_i(k)^3 - 5 \times 10^{-5}s_i(k)^2). \end{aligned}$$

First of all, we will give the various parameters used in the numerical simulation. The specific values of the parameters are presented below. The starting positions of nonlinear CAVs are chosen as $s_i(1) = [28.2 \ 20.2 \ 10 \ 0]$ with $i = 0, 1, 2, 3$. The velocity dynamics equations for the follower vehicle are similar to the leader dynamics equations and are omitted here. Similarly, the starting speeds of nonlinear CAVs are chosen as $\vartheta_i(1) = [2.08 \ 1.7 \ 1.7 \ 1.7]$. The sampling time T is selected as $T = 0.005$. The starting values of controller input $u_i(k)$ and PPD parameter $\varphi_i(k)$ are respectively chosen as $u_i(1) = 0$ and $\varphi_i(1) = 2$. In addition, it can be noticed by observing Figure 4 that, in the connected automated vehicle system model, the expected security distance is set to $d_{i,0} = [6 \ 16 \ 26]$. In the following, we will present the controller parameters of nonlinear CAVs, i.e., $\rho_i = [0.58 \ 0.49 \ 0.51]$, $\eta_i = [3.31 \ 2.55 \ 3.51]$, $\tau_i = [0.83 \ 0.86 \ 0.81]$, and $\lambda_i = [0.74 \ 0.68 \ 0.72]$. Then, the prescribed performance control parameters are set as

$\kappa_i = 0.0025$, $\Pi_i(\infty) = 0.50$, and $\Pi_i(1) = 3.5$. In addition, the parameters of attack duration time are selected as $\varepsilon_1 = 0.9$ and $\varepsilon_2 = 1.3$; one can obtain that $\epsilon < 3.49$. Then, we let $\epsilon = 3.19$ and $\Lambda_0 = 10$; then, we have $|\Lambda_a(0, 12000)| < 3771$. Therefore, the maximum duration time of DoS attacks is 18.855 s.

For the better highlighting of the superiority of the control scheme designed in this paper, here, a simulation comparison example [23] is used. Under the same controller parameters, model parameters, and aperiodic attacks, the control performance of the position and the speed tracking error can be illustrated through comparison with [23].

First of all, it follows from Figure 5a that the system's estimated PPD parameter $\hat{\varphi}_i(k)$ of three connected automated vehicles can reach agreement, which indicates that the unknown PPD parameter $\varphi_i(k)$ is exactly estimated through utilizing the developed PPD parameter estimation algorithm (24a) and (24b). In addition, the controller input (25) of this paper is exhibited in Figure 5b, which suggests that the system's controller inputs are progressively more consistent suffering from the influence of DoS attacks.

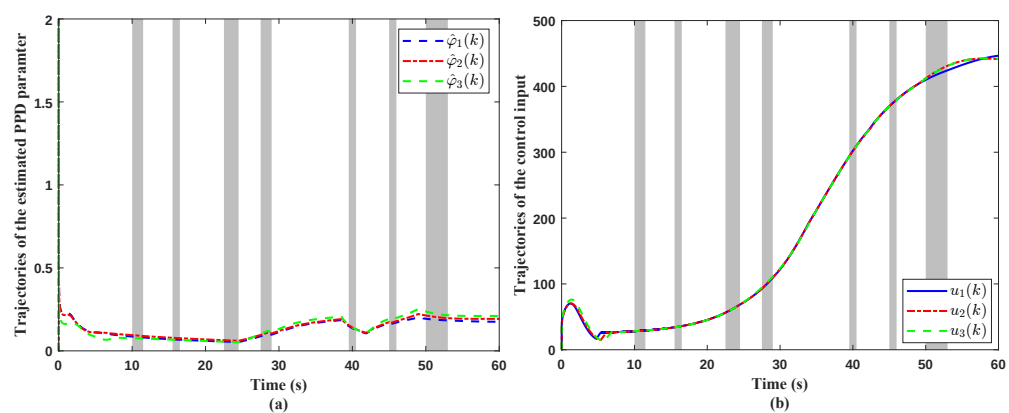


Figure 5. The trajectories of the estimated PPD parameter $\hat{\varphi}_i(k)$ (a) and controller input $u_i(k)$ (b) for the nonlinear connected automated vehicle system.

The comparison between the control scheme developed in this paper and the control scheme in [23] is given in Figures 6 and 7, in which the tracking trajectories of the position $s_i(k)$ and the position error $e_i(k)$ for nonlinear CAVs are illustrated. Through careful observation of Figure 6, it is possible to acquire that the follower vehicles can follow the trajectory of leaders in the existence of aperiodic DoS attacks and maintain a security distance between the vehicles, thus ensuring that no potential collision occurs. Nevertheless, collisions between vehicles may occur through using the control method [23]. Additionally, the tracking trajectories of the position tracking error $e_i(k) = s_0(k) - s_i(k) - d_{i,0}$ is illustrated in Figure 6. Through careful observation of Figure 6, it is possible to obtain that the position tracking error $e_i(k)$ is able to quickly converge to the predefined region, namely, the prescribed performance tracking control goal can be realized. However, by looking at Figure 7, it can be noticed that the position tracking error goes beyond the preset boundaries.

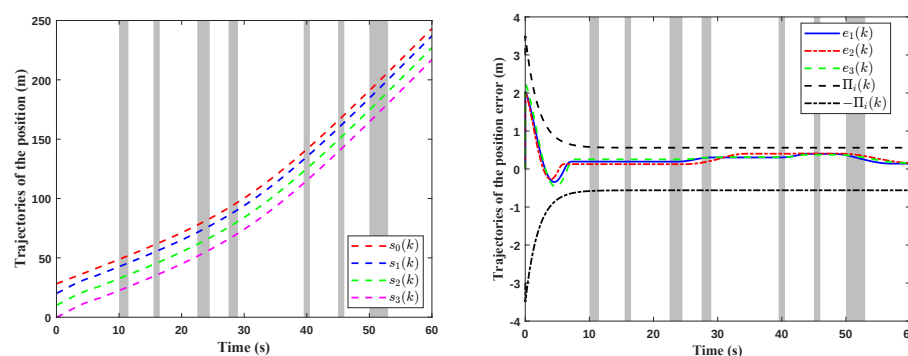


Figure 6. The trajectories of the position and position error with our method.

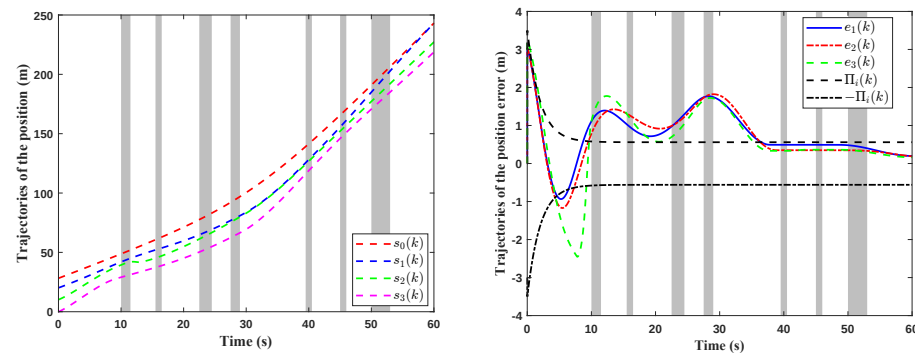


Figure 7. The trajectories of the position and position error with the method in [23].

Through observing Figure 7, one can conclude, at the initial moment, the initial value of the tracking error of the position is within the preset range. In the proposed method, the position tracking error converges, completing bounded convergence within 60 s and forming a smaller error around 0. However, using the method in [23] would result in the position tracking error exceeding the preset range and eventually converging to a larger error bound within 60 s.

Finally, a numerical comparison is given in Table 1 to demonstrate the superiority of the designed method. By looking at the table it can be obtained that our tracking error has a smaller value and has a shorter convergence time as compared to [23].

Table 1. The comparison of convergence effect.

Comparative Parameters	Our Method	Method in [23]	Unit
Tracking error $e_i(k)$	0.16	0.23	m
Starting convergence time	10	38	second (s)

5. Conclusions

This paper focuses on the model-free adaptive vehicular tracking control problem for nonlinear CAVs under prescribed performance constraint and aperiodic DoS attacks. The constrained output of nonlinear CAVs is converted to an unconstrained output through utilizing a strictly incremental function. Then, the output of the previous moment is utilized to mitigate the adverse influence generated by aperiodic DoS attacks. On the basis of the above two points, a novel model-free adaptive prescribed performance tracking control strategy is developed. Ultimately, the superiority of the designed control algorithm is presented through simulation. In future work, we will focus on problems for nonlinear CAVs such as sliding mode control, saturation, faults, and collision problems.

Author Contributions: Conceptualization, P.Z. and W.C.; methodology, Z.W. and W.C.; software, P.Z.; validation, Z.W. and W.C.; formal analysis, Z.W.; writing—original draft preparation, W.C.; writing—review and editing, P.Z. and Z.W.; supervision, W.C.; funding acquisition, W.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China under Grant 62273191, Grant U1966202, and Grant 62233015.

Data Availability Statement: Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. 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*, 2300–2302. [\[CrossRef\]](#)

2. Zhang, X.; Fang, S.; Shen, Y.; Yuan, X.; Lu, Z. Hierarchical velocity optimization for connected automated vehicles with cellular vehicle-to-everything communication at continuous signalized intersections. *IEEE Trans. Intell. Transp. Syst.* **2023**, *25*, 2944–2955. [\[CrossRef\]](#)
3. Liu, H.; Zhuang, W.; Yin, G.; Li, Z.; Cao, D. Safety-critical and flexible cooperative on-ramp merging control of connected and automated vehicles in mixed traffic. *IEEE Trans. Intell. Transp.* **2023**, *24*, 2920–2934. [\[CrossRef\]](#)
4. Ge, X.; Han, Q.-L.; Zhang, X.-M.; Ding, D. Communication resource-efficient vehicle platooning control with various spacing policies. *IEEE/CAA J. Autom. Sin.* **2023**, *11*, 362–376. [\[CrossRef\]](#)
5. Husain, S.S.; Al-Dujaili, A.Q.; Jaber, A.A.; Humaidi, A.J.; Al-Azzawi, R.S. Design of a Robust Controller Based on Barrier Function for Vehicle Steer-by-Wire Systems. *World Electr. Veh. J.* **2024**, *15*, 17. [\[CrossRef\]](#)
6. Li, Y.; Zhao, Y.; Tong, S. Adaptive fuzzy control for heterogeneous vehicular platoon systems with collision avoidance and connectivity preservation. *IEEE Trans. Fuzzy Syst.* **2023**, *31*, 3934–3943. [\[CrossRef\]](#)
7. Abbas, S.; Husain, S.; Al-Wais, S.; Humaidi, A. Adaptive Integral Sliding Mode Controller (SMC) Design for Vehicle Steer-by-Wire System. *SAE Int. J. Veh. Dyn. Stab. NVH* **2024**, *8*, 383–396. [\[CrossRef\]](#)
8. Che, W.-W.; Zhang, L.; Deng, C.; Wu, Z.-G. Hierarchical lane-changing control for vehicle platoons in prescribed performance. *Automatica* **2025**, *171*, 111972. [\[CrossRef\]](#)
9. Zhang, S.-Q.; Che, W.-W.; Deng, C. Observer-based event-triggered control for linear mass under a directed graph and dos attacks. *J. Control Decis.* **2022**, *9*, 384–396. [\[CrossRef\]](#)
10. Hong, Y.; Su, Y.; Cai, H. Internal Model Based Cooperative Robust Resilient Control Under DoS Attacks With Application to Vehicles Formation. *IEEE Trans. Ind. Inform.* **2024**, *early access*. [\[CrossRef\]](#)
11. Ren, Y.; Xie, X.; Nguyen, A.-T. Security control of autonomous ground vehicles under dos attacks via a novel controller with the switching mechanism. *IEEE Trans. Fuzzy Syst.* **2024**, *32*, 3669–3681. [\[CrossRef\]](#)
12. Zhao, N.; Zhang, H.; Shi, P. Observer-based sampled-data adaptive tracking control for heterogeneous nonlinear multi-agent systems under denial-of-service attacks. *IEEE Trans. Autom. Sci. Eng.* **2024**, *early access*. [\[CrossRef\]](#)
13. Luo, X.; Zhu, M.; Wang, X.; Guan, X. Detection and isolation of false data injection attack via adaptive kalman filter bank. *J. Control Decis.* **2024**, *11*, 60–72. [\[CrossRef\]](#)
14. Wang, Y.-M.; Li, Y.-X. Adaptive security control of time-varying constraints nonlinear cyber-physical systems with false data injection attacks. *J. Control Decis.* **2024**, *11*, 50–59. [\[CrossRef\]](#)
15. Yan, B.; Ni, J.; Zhong, Y.; Yu, D.; Wang, Z. Collision-Free Formation Control for Heterogeneous Multiagent Systems Under DoS Attacks. *IEEE Trans. Cybern.* **2024**, *54*, 6244–6255. [\[CrossRef\]](#)
16. Hou, Z.; Jin, S. Data-driven model-free adaptive control for a class of mimo nonlinear discrete-time systems. *IEEE Trans. Neural Netw.* **2011**, *22*, 2173–2188.
17. Bu, X.; Hou, Z.; Zhang, H. Data-driven multiagent systems consensus tracking using model free adaptive control. *IEEE Trans. Neural Netw. Learn. Syst.* **2017**, *29*, 1514–1524. [\[CrossRef\]](#)
18. Hou, Z.; Zhu, Y. Controller-dynamic-linearization-based model free adaptive control for discrete-time nonlinear systems. *IEEE Trans. Industrial Inform.* **2013**, *9*, 2301–2309. [\[CrossRef\]](#)
19. Hou, Z.; Jin, S. A novel data-driven control approach for a class of discrete-time nonlinear systems. *IEEE Trans. Control Syst.* **2010**, *19*, 1549–1558. [\[CrossRef\]](#)
20. Chen, R.Z.; Li, Y.X.; Hou, Z.S. Distributed model-free adaptive control for multi-agent systems with external disturbances and DoS attacks. *Inf. Sci.* **2022**, *613*, 309–323. [\[CrossRef\]](#)
21. Deng, C.; Jin, X.-Z.; Wu, Z.-G.; Che, W.-W. Data-driven-based cooperative resilient learning method for nonlinear mass under dos attacks. *IEEE Trans. Neural Netw. Learn. Syst.* **2023**, *35*, 12107–12116. [\[CrossRef\]](#) [\[PubMed\]](#)
22. Zhu, P.; Jin, S.; Bu, X.; Hou, Z. Distributed Data-Driven Control for a Connected Autonomous Vehicle Platoon Subjected to False Data Injection Attacks. *IEEE Trans. Autom. Sci. Eng.* **2023**, *21*, 7527–7538. [\[CrossRef\]](#)
23. Zhang, P.; Che, W.-W. Data-driven prescribed performance platooning sliding mode control under dos attacks. *Int. J. Robust Nonlinear Control* **2024**, *34*, 11581–11603. [\[CrossRef\]](#)
24. Zhou, Q.; Ren, Q.; Ma, H.; Chen, G.; Li, H. Model-Free Adaptive Control for Nonlinear Systems Under Dynamic Sparse Attacks and Measurement Disturbances. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2024**, *71*, 4731–4741. [\[CrossRef\]](#)
25. Bechlioulis, C.P.; Rovithakis, G.A. Robust adaptive control of feedback linearizable mimo nonlinear systems with prescribed performance. *IEEE Trans. Autom. Control* **2008**, *53*, 2090–2099. [\[CrossRef\]](#)
26. Zhang, L.; Che, W.-W.; Chen, B.; Lin, C. Adaptive fuzzy output-feedback consensus tracking control of nonlinear multiagent systems in prescribed performance. *IEEE Trans. Cybern.* **2022**, *53*, 1932–1943. [\[CrossRef\]](#)
27. Shi, S.-N.; Li, Y.-X. Event-based adaptive asymptotic tracking control of nonlinear time-varying systems with prescribed performance. *J. Control Decis.* **2023**, *10*, 355–364. [\[CrossRef\]](#)
28. Liu, Y.; Wang, X.; Chen, Z.; Li, L. Adaptive Event-Triggered Path Tracking Control with Proximate Appointed-Time Prescribed Performance for Autonomous Ground Vehicles. *IEEE Trans. Ind. Electron.* **2024**, *early access*. [\[CrossRef\]](#)
29. Liu, D.; Yang, G.-H. Data-driven adaptive sliding mode control of nonlinear discrete-time systems with prescribed performance. *IEEE Trans. Syst. Man Cybern. Syst.* **2017**, *49*, 2598–2604. [\[CrossRef\]](#)
30. Hou, M.; Wang, Y. Data-driven adaptive terminal sliding mode control with prescribed performance. *Asian J. Control* **2021**, *23*, 774–785. [\[CrossRef\]](#)

31. Liu, D.; Zhou, Z.-P.; Li, T.-S. Data-driven bipartite consensus tracking for nonlinear multiagent systems with prescribed performance. *IEEE Trans. Syst. Man Cybern. Syst.* **2023**, *53*, 3666–3674. [[CrossRef](#)]
32. Esmaeili, B.; Salim, M.; Baradarannia, M. Predefined performance-based model-free adaptive fractional-order fast terminal sliding-mode control of MIMO nonlinear systems. *ISA Trans.* **2022**, *131*, 108–123. [[CrossRef](#)] [[PubMed](#)]
33. Feng, S.; Tesi, P. Resilient control under denial-of-service: Robust design. *Automatica* **2017**, *79*, 42–51. [[CrossRef](#)]
34. Xu, D.; Jiang, B.; Shi, P. A novel model-free adaptive control design for multivariable industrial processes. *IEEE Trans. Ind.* **2014**, *61*, 6391–6398. [[CrossRef](#)]
35. Sharma, N.K.; Roy, S.; Janardhanan, S. New design methodology for adaptive switching gain based discrete-time sliding mode control. *Int. J. Control* **2021**, *94*, 1081–1088. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.